



November 19, 2025

Board Oversight of Compliance, Major Investigations, and Interactions with Enforcers

GIBSON DUNN

MCLE Certificate Information

MCLE Certificate Information

- Approved for 1.0 hours General PP credit.
- CLE credit form must be submitted by **Wednesday, November 26th**.
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_cCOUTTKWEWMHZ54
 - Most participants should anticipate receiving their certificate of attendance in four to eight weeks following the webcast.
- **Please direct all questions regarding MCLE to CLE@gibsondunn.com.**

Presenters



Barry H. Berke

Partner
New York
bberke@gibsondunn.com



Winston Y. Chan

Partner
San Francisco
wchan@gibsondunn.com



Jina L. Choi

Partner
San Francisco
jchoi@gibsondunn.com



Nicola T. Hanna

Partner
Los Angeles
nhanna@gibsondunn.com



F. Joseph Warin

Partner
Washington, D.C.
fwarin@gibsondunn.com

Agenda

01 **Introductory Remarks**

02 **Board Oversight Responsibilities**

03 **Oversight of Compliance Programs**

04 **Interactions with Enforcement Authorities**

05 **Oversight of Major Matters**

06 **Emerging Areas of Risk**

Introductory Remarks

01

Board Oversight Responsibilities

02

Board Oversight Responsibilities

Caremark

- ***In re Caremark Int'l Inc. (Del. Ch. 1996)***: Directors have a duty to ensure **adequate corporate oversight systems are in place**.
 - The board must “exercise a good faith judgment that the corporation’s information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility.”
- Directors may be held liable if they have:
 - (1) Completely **failed to implement** reporting or information systems or controls; or
 - (2) **Consciously failed to monitor or oversee** existing controls, thus disabling themselves from being informed of risks or problems.

Source: *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959, 970 (Del. Ch. 1996).

Board Oversight Responsibilities *Liability for Business Risk*

- Since 1996, the *Caremark* good faith duty to monitor risk has been addressed in hundreds of cases.
- The *Caremark* duty may not be used to second-guess a well-informed board's business decisions, including decisions regarding risk-taking.

In re Citigroup
(Del. Ch. 2009)

“[T]he mere fact that a company takes on business risk and suffers losses – even catastrophic losses – does not evidence misconduct and without more, is not a basis for personal director liability.”

*In re
ProAssurance*
(Del. Ch. 2023)

- “Evaluating business risk is ‘the quintessential board function.’ So long as the challenged conduct is lawful, directors have broad discretion to advance the corporation’s interests as they see fit.”

Board Oversight Responsibilities

Recent Cases

Marchand (Del. 2019)

- Reversed dismissal of complaint against board of ice cream manufacturer [Blue Bell Creameries](#) for failing to oversee food safety and compliance issues involving a listeria outbreak and the death of three customers.
- The Court focused on the board's alleged [failure to implement any system for overseeing and monitoring mission-critical aspects](#) of the company's business.

In re Clovis (Del. Ch. 2019)

- Court declined to dismiss *Caremark* claim that arose when [Clovis Oncology](#) withdrew its only product from FDA consideration after disappointing clinical trials.
- The Court found that the board received reports on the drug's development but [ignored multiple warning signs that management was inaccurately reporting the drug's efficacy](#).

In re Boeing (Del. Ch. 2021)

- Plaintiffs stated a *Caremark* claim against the [Boeing](#) board as a result of 737 MAX airplane crashes in 2018 and 2019.
- In 2022, Boeing settled the claim for approximately \$237.5 million.

Board Oversight Responsibilities *Recent Cases*

- On September 29, 2025, the Delaware Court of Chancery declined to dismiss a *Caremark* claim arising from a \$191 million consent order with the CFPB related to improper overdraft fee practices at [Regions Bank](#).
- The court allowed plaintiffs to pursue claims that the Board failed to properly respond to a red flag, namely, a whistleblower complaint alleging retaliation for calling attention to the Bank's illegal overdraft fees.

“Everyone knows that delay can be intentional and a tactic to avoid the consequences of acting appropriately. . . **Consciously delaying actions that a Board knows to be illegal supports an inference of bad faith.**”

“Hiring counsel to advise regulatory risk is a good thing. But . . . **[m]erely hiring an attorney in response to a red flag . . . does not provide the absolution Defendants seek.**”

Board Oversight Responsibilities *Recent Cases*

- On September 2, 2025, the Delaware Court of Chancery declined to dismiss a *Caremark* claim arising from the bankruptcy of [Teligent](#), a generic pharmaceutical company.
- The court dismissed plaintiffs' red flags claim but allowed plaintiffs' claims that the board failed to implement information systems over mission-critical FDA compliance.

Teligent allegedly lacked:

- A board committee responsible for regulatory compliance;
- Processes and protocols requiring management to keep the board apprised of compliance risks; and
- Training protocols designed to inform employees of central compliance risks.

“This is about as close to an utter failure as it gets.”

Oversight of Compliance Programs

03

Board Oversight Responsibilities

What Should Boards Focus on?

Three general principles can be extracted from the caselaw:

- Courts have focused on boards' **monitoring of key enterprise risks** affecting a corporation's "mission critical" components.
- Oversight violations are typically found where companies **violate affirmative law or regulatory mandates**.
- Boards should be **particularly attentive** when there **are red flags** and issues arise.

Board Oversight Responsibilities

What Should Boards Focus on?

Where Have Boards Fallen Down?

- Board was not informed
- Failure to act on red flags
- Failure to have systems for mission critical issues
 - No committee
 - Lack of meetings
 - Lack of updates

Board Oversight Responsibilities

What Should Boards Focus on?

What Do Enforcers Expect?

- Tone at the top
- Devote resources
- Experience/expertise
- Chief Compliance Officer with direct path to the board

Board Oversight Responsibilities

Key Takeaways

Key Takeaways:

- Identify “mission-critical” risks
- Delegate responsibility for oversight
- Set regular reporting schedule
- Proactively address “Red Flags”
- Remain vigilant

Practical Considerations

Ensure regular compliance program reporting.

- **Annual reporting** about staffing, resources, and structure of the compliance program.
- **Prompt reporting** about material compliance issues as they develop (e.g., material allegations involving senior management).
- **Regular reporting** to provide data and trend information about use of reporting mechanisms. These reports often contain:
 - Distribution of compliance issue types;
 - Trends for how long it takes to initiate and complete review;
 - Size and age of unreviewed backlog;
 - Size, use, and trends of hotline reports; and
 - Overall trends for the compliance program.

Interactions with Enforcement Authorities

04

Whistleblower and Self-Disclosure Programs

2024 saw several key changes to voluntary disclosure and whistleblowing programs, including:

- The launch of the Criminal Division **Corporate Whistleblower Awards Pilot Program** in August 2024, providing corporate whistleblowers with monetary rewards if a disclosure ends with forfeiture under certain conditions;
- DOJ Criminal Division's new **Pilot Program on Voluntary Self-Disclosures for Individuals**, which offers NPAs as an incentive for individuals involved in misconduct to self-disclose, subject to certain conditions;

Questions remain around how DOJ will promote or leverage these programs in the second Trump Administration.

- **Individual whistleblower programs** launched by twelve United States Attorneys' Offices.

The first Trump administration saw an increased role for USAOs, and individual tip line-type programs with rewards have long been used by law enforcement agencies, even without explicit bases in statutes.

Whistleblower Programs: DOJ Criminal Division

Announced in March and launched in August 2024, DOJ Criminal Division's **Corporate Whistleblower Awards Pilot Program** aims to fill the gaps in existing whistleblower programs by providing incentives to whistleblowers not covered by other frameworks (such as those administered by the SEC, CFTC, etc.).

Under this three-year pilot program:

- Whistleblowers are eligible for awards in cases resulting in forfeiture exceeding **\$1 Million**.
- Open to whistleblowers who have “**minimally**” participated or are “**least culpable**” in the scheme.
 - Prohibits awards to individuals who “**meaningfully participated in the criminal activity**,” even if they self-disclose.
- Whistleblowers must provide “**original information**” to the DOJ about cases involving:
 - (1) Certain crimes involving financial institutions, from traditional banks to cryptocurrency businesses;
 - (2) Foreign corruption involving misconduct by non-issuer companies;
 - (3) Domestic corruption involving misconduct by companies; or
 - (4) Health care fraud schemes involving private insurance plans.
- Companies can still be eligible for “**voluntary self-disclosure**” credit under the Corporate Enforcement Policy if they disclose the misconduct within 120 days of the whistleblower report.

This new program may create a “**race to the DOJ**” between corporations and individuals. Thus, corporations should consider:

- Maintaining strong internal controls systems to find and remediate misconduct internally; and
- Strengthening internal reporting tools for employees, third parties, and contractors.

“Early signs indicate” DOJ’s “newly consistent and transparent programs are working.”

Principal Associate Deputy Attorney General Marshall Miller, **August 2024**

Whistleblower Programs: SEC



Top 10 Whistleblower Awards

As of the end of fiscal year 2023, a total of almost \$2 billion had been awarded to nearly 400 whistleblowers through the SEC's whistleblower award program.

Here are the 10 largest awards issued to date...

By Award Amount

Listed by amount of each award issued:

- [\\$279 million](#) - May 5, 2023
- [\\$114 million](#) - Oct. 22, 2020
- [\\$110 million](#) - Sept. 15, 2021
- [\\$82 million](#) - Aug. 23, 2024
- [\\$50 million](#) - April 15, 2021
- [\\$50 million](#) - March 19, 2018
- [\\$50 million](#) - June 4, 2020
- [\\$39 million](#) - Sept. 6, 2018
- [\\$37 million](#) - Dec. 19, 2022
- [\\$37 million](#) - July 26, 2024

By Covered Action

Listed by total amount awarded under each covered action:

- [\\$279 million](#) - May 5, 2023
- [\\$114 million](#) - Oct. 22, 2020
- [\\$114 million](#) - Sept. 15, 2021
- [\\$104 million](#) - Aug. 4, 2023
- [\\$98 million](#) - Aug. 23, 2024
- [\\$83 million](#) - March 19, 2018
- [\\$54 million](#) - Sept. 6, 2018
- [\\$50 million](#) - April 15, 2021
- [\\$50 million](#) - March 26, 2019
- [\\$50 million](#) - June 4, 2020

Mitigation: Increasing Importance of Self- Reporting

Corporate Enforcement & Voluntary Self Disclosure Policy, Department of Justice Criminal Division

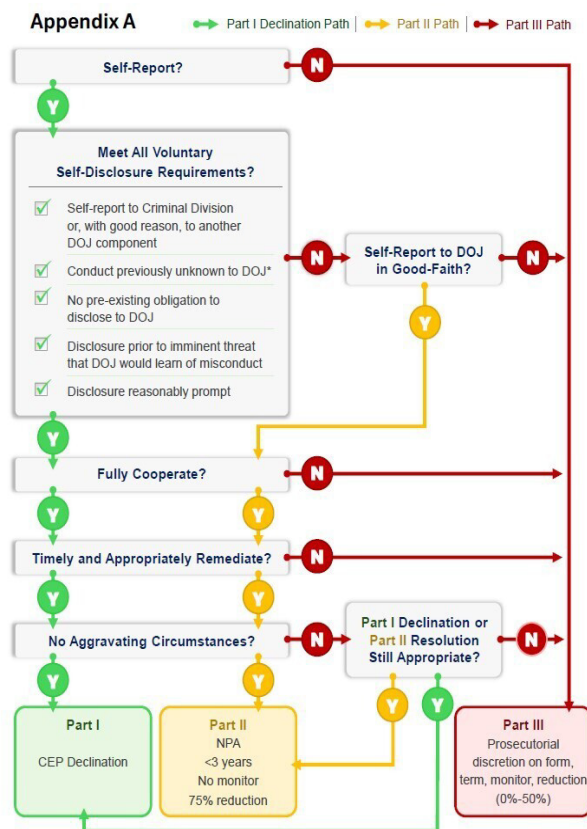
In May 2025, DOJ revised the Corporate Enforcement Policy to allow companies to better anticipate outcomes when self-reporting—with a flowchart.

Under the updated Corporate Enforcement Policy, DOJ's Criminal Division will publicly decline to prosecute a company for criminal conduct when:

1. The company voluntarily self-disclosed the misconduct to the Criminal Division, without a preexisting obligation to do so;
2. The company fully cooperates with the Criminal Division's investigation;
3. The company timely and appropriately remediated the conduct; and
4. There are no aggravating circumstances.

In instances of “near miss self-disclosures” or where there are aggravating (but not egregious) circumstances, DOJ will provide a Non-Prosecution Agreement for less than three years, without a monitorship, and with a 75% reduction off of the low end of the USSG fine range.

For resolutions in other cases, there is a presumption that any sentencing reduction will be taken from the low end of the Guidelines.



Practical Considerations for Public Investigations

Be prepared for investigations by authorities.

- Identify and prioritize key business processes and functions.
- Consider potential operational, financial, and reputational risks to critical processes.
- Evaluate likelihood and impact of those risks.
- Assess whether internal reporting channels are adequate in design and implementation.

Practical Considerations for Public Investigations

Be proactive in organizing response to investigations.

- Define a core, coordinating group of key stakeholders that centralizes the company's decisionmaking and response.
- Is a comprehensive plan in place for a public investigation?
 - Protocol that establishes escalation channels to avoid confusion and mitigate risk of compounding issues.
 - Establish an internal communication and decision-making tree.
 - Set up a mechanism to coordinate on a daily basis.
 - Set up a process that will best protect the attorney-client privilege.
 - Consider whether to provide counsel to the board and executives.
- Periodic training on the protocol to all relevant audiences is critical.

Oversight of Major Matters

05

Practical Considerations

Information must get to the board.

- The board should expect a routine flow of information and reports on mission critical components of the business.
 - Information flows may vary depending on developments and significance.
- A process should be developed to require management to deliver periodic reports to the board on mission critical items.
- Sometimes not appropriate to wait until the next regularly scheduled board meeting.
 - Failure to escalate timely can reflect poorly on the board and management, with the benefit of 20/20 hindsight.

Practical Considerations

Use board committees for oversight.

- Oversight of compliance programs and major matters can be integrated into the role of an already-standing committee focused on particular risks or the board as a whole.
 - This should be properly documented, such as via a board resolution or amendment to the appropriate committee charter.
 - A generic mandate that a committee be in charge of “risk oversight” will be less effective in defeating a *Caremark* claim than a more specific mandate focused on mission-critical risks tailored to the organization.
- Many companies assign the audit committee with general risk oversight.
 - Consider if doing so is appropriate in light of:
 - Already busy agenda and mandate of the audit committee; and
 - Possibility that oversight of mission critical components gets lost or overshadowed by oversight of financial risks.

Practical Considerations

Regularly discuss mission critical items.

- The board or assigned standing committee should **document its processes**, such as through a calendar, issue tracking document, and minutes.
- The board or assigned standing committee should regularly engage in discussions regarding mission critical components.
 - Discussions should occur on-the-record during regularly scheduled board or committee meetings with minutes and proper documentation.
 - When reasonably required, board members should not shy away from asking for additional materials and information from management and advisors.
 - Discussions should be concrete – aim for crisp discussions around specific mission critical areas of concern and mitigating steps.

Practical Considerations

Ensure that major matters are escalated to the board.

- Maintain a protocol outlining when major investigations and compliance matters should be escalated to the board.
 - The protocol should list **escalation triggers** and when in an investigation they usually occur.
 - The protocol should define when investigations should be **communicated to the audit committee or to the full board**.
- Where misconduct implicates **senior management or critical governance issues**, it is important to ensure that directors oversee the matter and receive updates to assist them in fulfilling fiduciary oversight duties.

Practical Considerations

Be proactive and engaged if “corporate trauma” occurs.

- If a significant incident occurs, the board should be engaged and demonstrate proactive involvement.
 - A recurring theme in negative *Caremark* decisions is the appearance the board was disengaged and not proactive with management regarding an escalating crisis.
 - In the *Boeing* case, the Court highlighted the board’s apparent passivity following the air crashes, its perceived uncritical reliance on intermittent management reports, and its apparent failure to press for information until well after the second aircraft crash.
- Full engagement at the time of crisis is critical. But it is not a cure all.
 - Establish a core, coordinating group of key stakeholders that centralizes the company’s decisionmaking and response.
 - Define a protocol establishing escalation channels and roles during a crisis.

Emerging Areas of Risk

06

Emerging Areas of Risk

Monitor enforcement priorities and emerging areas of risk. For example:

Cybersecurity

DEI

Trade

Emerging Areas of Risk *Cybersecurity*

Cybersecurity

- The Delaware Chancery Court has recently dismissed cases alleging Caremark claims involving cybersecurity breaches.
 - *Construction Industry Laborers Pension Fund v. Bingle (2022)* concerned a data breach at SolarWinds resulting in a massive leak of its customers' personal information.
 - *Firemen's Ret. Sys. of St. Louis v. Sorenson (2021)* concerned Marriott's data breach that exposed the personal information of up to 500 million guests.
- The courts emphasized that the boards' conduct was not in "bad faith": each board had established reporting and monitoring systems (albeit arguably flawed) and their alleged inattention to cybersecurity issues was not intentional (though perhaps negligent).

Emerging Areas of Risk *Cybersecurity*

SEC Cybersecurity Disclosure Rule

- Adopted July 26, 2023, effective December 2023
- Public companies must disclose material cyber incidents within four business days of determining materiality.
 - Ransomware attacks
 - Data breaches with customer or financial data exposure
 - Incidents affecting operational integrity
- Item 106 of Reg S-K
 - Cybersecurity Risk Management and Strategy
 - Cybersecurity Governance

Emerging Areas of Risk *Cybersecurity*

Cybersecurity

- DOJ [Data Security Program](#) provisions went into effect on October 6, 2025. They require companies engaged in transactions involving bulk U.S. sensitive personal data or government-related data to meet ongoing compliance obligations, including audits, reporting and certification requirements, and long-term recordkeeping.
- DoD [Cybersecurity Maturity Model Certification Requirements](#) went into effect on November 10, 2025, imposing new cybersecurity requirements, assessments, and certifications to evaluate contractors' information security programs.
- DOJ's cybersecurity FCA theories focus on compliance and certification with standards. Potential DOJ theories and allegations include knowingly:
 - [Failing to meet](#) government-imposed cybersecurity standards and requirements;
 - [Misrepresenting](#) company's own security controls or capabilities, whether or not government-required; and
 - [Failing to report](#) known cyber incidents.

Emerging Areas of Risk *Cybersecurity*

Life sciences
corporation
\$9.8 million
(July 2025)

- Alleged sale to federal agencies of genomic sequencing systems containing **cybersecurity vulnerabilities**.
- Alleged false **representations of compliance** with cybersecurity standards.

Defense contractor
and private equity firm
\$1.75 million
(July 2025)

- Alleged **failure to implement** required cybersecurity controls.
- Alleged **failure to limit access** to sensitive defense information.

Research institution
\$875,000
(September 2025)

- Alleged **failure to meet cybersecurity requirements** in connection with Air Force and DARPA contracts.
- Alleged submission of false summary-level cybersecurity assessment score to DoD.

Emerging Areas of Risk *DEI*

DEI

- Executive Order 14173, [Ending Illegal Discrimination and Restoring Merit-Based Opportunity](#), orders “all agencies to enforce our longstanding civil-rights laws and to combat illegal private-sector DEI preferences, mandates, policies, programs, and activities.”
- [DOJ guidance](#) from July 30, 2025, provides a non-exhaustive list of policies and practices DOJ considers unlawful, including:
 - Programs that grant preferential treatment based on protected characteristics; and
 - Policies that use facially-neutral proxies for protected characteristics.
- In May 2025, DOJ announced the [Civil Rights Fraud Initiative](#) to use the False Claims Act to investigate and pursue claims against recipients of federal funds that knowingly violate the civil rights laws.

Emerging Areas of Risk DEI

DOJ's new guidance
regarding DEI focuses
on several features:

Preferential treatment based on
protected characteristics

Facially neutral policies that either:
(1) replicate consideration of
protected characteristics; or
(2) are implemented with intent to
advantage or disadvantage


Trainings that either:
(1) exclude or penalize based on
protected characteristics; or
(2) create an
“objectively hostile” work
environment



Office of the Attorney General
Washington, D. C. 20530

March 21, 2025

MEMORANDUM FOR ALL FEDERAL AGENCIES

FROM: THE ATTORNEY GENERAL 
SUBJECT: IMPLEMENTATION OF EXECUTIVE ORDERS 14151 AND 14173:
ELIMINATING UNLAWFUL DEI PROGRAMS IN FEDERAL
OPERATIONS

I. INTRODUCTION

This memorandum provides guidance to all federal agencies regarding compliance with Executive Order 14151 of January 20, 2025 (Ending Inefficient and Wasteful Government DEI Programs and Preferential Treatment) and Executive Order 14173 of January 21, 2025 (Ending Illegal Discrimination). In those Executive Orders, President Trump announced the termination of race- and sex-based preference programs operating under the banner of “diversity, equity, and inclusion” (DEI) throughout the federal government. As the President explained, “dangerous, demeaning, and immoral race- and sex-based preferences under the guise of so-called ‘diversity, equity, and inclusion’ violate the civil rights laws of this country and will no longer be tolerated—least of all within our own government.” Executive Order 14173 § 1.

This memorandum outlines core legal principles that must guide agency compliance with efforts to dismantle unlawful DEI initiatives, with more specific implementation instructions to follow.

II. FRAMEWORK

Constitutional Imperatives

The Equal Protection Clause of the Constitution establishes the foundational principle that government may never discriminate based on protected characteristics, including race, except in rare circumstances. As the Supreme Court articulated in *Students for Fair Admissions, Inc. v. President & Fellows of Harvard College* (“SFFA”), 600 U.S. 181, 206 (2023), the “core purpose” of the Equal Protection Clause is to “do away with all governmentally imposed discrimination based on race.” The Court further emphasized that “eliminating racial discrimination means eliminating *all* of it.” *Id.* (emphasis added). The Supreme Court has accordingly “forcefully rejected the notion that government actors may intentionally allocate

Emerging Areas of Risk *DEI*

DEI

- Multiple federal agencies are [actively investigating DEI practices](#).
- Recent [higher education](#) resolution agreements incorporate DEI-related provisions.
 - Several major institutions have entered agreements that they “will not provide benefits or advantages to individuals on the basis of protected characteristics.”
- DOJ has recently initiated a series of [DEI-related FCA investigations](#). These investigations are in early stages.

Emerging Areas of Risk *Trade*

Trade

- Tariffs are at historically high levels—the [highest since the 1930s](#).
- Tariffs fluctuate based on [Administration priorities](#) and whether [deals](#) exist with specific countries.
- Tariffs are targeted at [specific imports and industries](#) (e.g., steel, aluminum, auto parts), and at [specific countries](#) and regions (e.g., China, Canada).
- The sheer magnitude of these tariffs creates a risk of DOJ scrutiny based on [allegations of avoidance](#).

Emerging Areas of Risk *Trade*

Trade

- In August 2025, DOJ launched the [Trade Fraud Task Force](#) to coordinate between its Civil and Criminal Divisions and DHS to “aggressively pursue enforcement actions” under the FCA and the Tariff Act, along with criminal prosecutions.
- Prior to the announcement, in July 2025, Cadence Design Systems pled guilty to criminal charges alleged by the DOJ Counterintelligence and Export Control Section for exporting semiconductor design tools to a Chinese military university.
- Cadence also resolved a parallel civil investigation into the same matter with BIS and agreed to pay \$95 million. Cadence will pay over \$140 million in these resolutions.

Emerging Areas of Risk Trade

Potential Liability Extends Beyond the Importer of Record to the Domestic Buyer of the Imported Good

- Courts have **rejected** the argument that only the “importer of record” can be liable under the FCA for avoiding customs duties.

Ultimate importer “**was not exempt from the obligation to pay the government** just because [it] and the Non-parties agreed that the Non-parties were the sole ‘importer of record.’”
U.S. ex rel. Henig v. Amazon, 2025 WL 27736, at *10 (S.D.N.Y. 2025).

Liability can attach to a party that “**caused others**” including “foreign manufacturers[and] Customs broker[s] . . . **to present false information to the Government**” to lower duties owed. *U.S. ex rel. Taylor v. GMI USA Corp.*, 714 F. Supp. 3d 275, 290 (S.D.N.Y. 2024).

- In 2017, DOJ entered into a \$1 million settlement with a U.S.-based wholesaler that it alleged “**repeatedly ignored warning signs**” that its China-based importer “was engaged in a scheme to underpay customs duties owed on the imported garments.”

Emerging Areas of Risk *Trade*

**Procurement and
logistics firm
\$22 million
(September 2020)**

Alleged **misclassification of construction materials** by “misrepresenting the nature, classification, and valuation of imported merchandise, as well as the applicability of free trade agreements.”

**Wiring and power
distribution
companies
\$10 million
(August 2024)**

Alleged submission to customs broker of invoices that **undervalued goods** imported from China by as much as 70%.

**Flooring company
\$8.1 million
(March 2025)**

Alleged submission to customs officials of invoices that **falsely represented country of origin**.

Upcoming December Programs

2025/2026 White Collar Webcast Series

Date and Time	Program	Registration Link
Monday, December 1, 2025 9:00 AM – 10:00 AM PT 12:00 PM – 1:00 PM ET	Tariff Evasion Presenters: Matthew Axelrod, Nicola Hanna, Poonam Kumar, Chris Timura, Adam Smith	Event Details
Wednesday, December 3, 2025 9:00 AM – 10:00 AM PT 12:00 PM – 1:00 PM ET	Between DC and the Districts: Charting the US Attorney Landscape Presenters: Matthew Axelrod, Doug Fuchs, Nicola Hanna, Debra Wong Yang	Event Details
Thursday, December 4, 2025 9:00 AM – 10:30 AM PT 12:00 PM – 1:30 PM ET	Understanding the Trump Administration’s Impact on Government Contractors and Grant Recipients Presenters: Stuart Delery, Lindsay Paulin, Jake Shields	Event Details
Tuesday, December 9, 2025 9:00 AM – 10:30 AM PT 12:00 PM – 1:30 PM ET	Protecting Your Executives – Enforcement Against Individuals in the Trump Administration Presenters: Jordan Estes, Doug Fuchs, Nicola Hanna, Dani James, Mike Martinez	Event Details
Thursday, December 11, 2025 9:00 AM – 10:00 AM PT 12:00 PM – 1:00 PM ET	Navigating DOJ’s M&A Safe Harbor: Policy, Practice, and Strategic Implications Presenters: Matthew Axelrod, Michael Farhang, Alex Fine, Patrick Stokes	Event Details

GIBSON DUNN

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome. © 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at [gibsondunn.com](https://www.gibsondunn.com).