September 24, 2024

False Claims Act Enforcement Developments and Trends: Cybersecurity

Winston Y. Chan
Stephenie Gosnell Handler
Melissa L. Farrar
Michael R. Dziuban

GIBSON DUNN

MCLE CERTIFICATE INFORMATION

MCLE Certificate Information

- Approved for 1.0 hour General PP credit.
- CLE credit form must be submitted by **Tuesday, October 1st.**
- Form Link: https://gibsondunn.qualtrics.com/jfe/form/SV_6VTqGbvMo1bdEeW
  - 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.**

OUR SPEAKERS

Winston Y. Chan

Partner; Co-Chair, White Collar Defense and Investigations; False Claims Act/Qui Tam Defense, San Francisco

Winston serves as co-chair of the firm's White Collar Defense and Investigations practice group, and also its False Claims Act/Qui Tam Defense practice group. He leads matters involving government enforcement defense, internal investigations and compliance counseling, and regularly represents clients before and in litigation against federal, state and local agencies, including the U.S. Department of Justice, Securities and Exchange Commission and State Attorneys General.

Prior to joining the firm, Winston served as an Assistant United States Attorney in the Eastern District of New York, where he held a number of supervisory roles and investigated a wide range of corporate and financial criminal matters.

Stephenie Gosnell Handler

Partner, Washington, D.C.

Stephenie advises clients on complex legal, regulatory, and compliance issues relating to international trade, cybersecurity, and technology matters. Stephenie's legal advice is deeply informed by her operational cybersecurity and in-house legal experience at McKinsey & Company, and also by her active duty service in the U.S. Marine Corps.

Stephenie returned to Gibson Dunn as a partner of the Washington, D.C. office after serving as Director of Cybersecurity Strategy and Digital Acceleration at McKinsey & Company. Stephenie frequently advised at the intersection of cybersecurity, technology, and data and export control and sanctions requirements.

Melissa L. Farrar

Partner, Washington, D.C.

Melissa's practice focuses on white collar defense, internal investigations, and corporate compliance. She represents and advises multinational corporations in internal and government investigations on a wide range of topics, including the U.S. Foreign Corrupt Practices Act, the False Claims Act, anti-money laundering, and accounting and securities fraud, including defending U.S. and global companies in civil and criminal investigations pursued by the U.S. Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC"). Melissa also has experience representing U.S. government contractors in related suspension and debarment proceedings.

Michael R. Dziuban

Associate, Washington, D.C.

Michael represents clients in white collar defense and civil enforcement matters, including investigations and lawsuits under the False Claims Act. He has advised government contractors, technology companies, health care companies, and individual executives in various stages of FCA enforcement opposite both government agencies and *qui tam* relators. Michael also has guided clients through government and internal investigations under anti-corruption and anti-money laundering laws, advised clients in government contracts disputes, and counseled companies on their corporate compliance programs.

AGENDA

The False Claims Act

- FCA Basics
- Recent Legal Developments
- Enforcement Priorities & Trends

Government Contracting

- Contractor Cybersecurity: Overview & Cyber Incident Reporting

Health Care & Cybersecurity

- Risks for Device Manufacturers

FCA Cybersecurity Developments

- Recent Enforcement Actions

THE FALSE CLAIMS ACT
FCA BASICS

FCA BASICS

The False Claims Act (FCA)

- The FCA, 31 U.S.C. §§ 3729–3733, is the federal government's **primary tool for combating fraud** against government agencies and programs.
- The FCA provides for recovery of **civil penalties and treble damages** from any person who knowingly submits or causes the submission of false or fraudulent claims to the United States for money or property.
- The Attorney General, through prosecutors at Main DOJ and U.S. Attorney's Offices, investigates and pursues FCA cases—working in close coordination with federal agencies.
- DOJ devotes substantial resources to pursuing FCA cases—and to considering whether FCA matters merit parallel criminal investigations.

"It seems quite clear that the objective of Congress was broadly ***to protect the funds and property of the Government from fraudulent claims*** …."

Rainwater v. United States, 356 U.S. 590 (1958)

FCA BASICS

The False Claims Act (FCA)

Elements of an FCA case:

- **Falsity**: A request for payment (claim) that is false or fraudulent.
  - Factual falsity: Billing for goods or services that were not correctly described or not provided at all.
  - Legal falsity: When a claim is based on a false representation of compliance, express or implied, with statutory, regulatory, or contractual requirements.
- **Materiality**: The falsity of the claim was material to the government's payment of the claim.
- **Scienter**: The false claim was submitted with knowledge of its falsity—in the form of "actual knowledge," "deliberate ignorance," or "reckless disregard."
- **Causation and harm**: The false claim caused the government to suffer financial harm (i.e., payment of the claim).

To succeed, the plaintiff—either the government or a whistleblower—must prove each of the above by a ***preponderance of the evidence*.**

FCA BASICS

Factual Falsity

- False billing (e.g., goods or services not provided)
- Overbilling (e.g., upcoding)

Legal Falsity

- Express certification of compliance with legal requirements
- Submission of claim with representations rendered misleading as to goods/services provided

Promissory Fraud / Fraud in the Inducement

- Obtaining a contract through false statements or fraudulent conduct
- *United States ex rel. Marcus v. Hess*, 317 U.S. 537 (1943) (claims by contractors who colluded on bids)

Reverse False Claims

- Improper avoidance of obligation to pay money to the government
- Retention of government overpayment

FCA BASICS

Qui Tam Provisions

- The FCA's *qui tam* provisions enable so-called "relators" to bring cases in the government's name and receive as much as **30%** of the recovery or judgment.
- The government may intervene, but an increasing number of cases are pursued without government intervention (but often with a government statement of interest).
- DOJ has broad authority to dismiss *qui tam* suits.
- Whistleblower protections, 31 U.S.C. § 3730(h), protect employees and others (e.g., contract workers) who report fraud.
  - Relief under Section 3730(h) may include double back pay and interest on back pay; reinstatement (at same level); and costs and attorneys' fees.
  - Case law continues to develop, e.g., around meaning of anti-retaliation provision's causation language ("because of").

"In short, sir, I have based the [*qui tam* provision] upon the old-fashioned idea of holding out a temptation and '***setting a rogue to catch a rogue***,' which is the safest and most expeditious way I have ever discovered of bringing rogues to justice."

Statement of Senator Howard, Cong. Globe, 37th Cong. 955-56 (1863)

FCA BASICS

Damages and Civil Penalties

- **Treble damages** are traditionally calculated by multiplying the government's loss by three (e.g., if the government was charged $100 for goods not received, damages would be $300)
- But the damages calculation can be much more complicated (and less certain) when the government receives goods or services it considers deficient or when there is a "false certification" or "promissory fraud."
- In addition to damages, there is **a per-violation civil penalty**:
  - Current range, per final rule issued in February 2024: **$13,946 to $27,894** per violation occurring after November 2, 2015 and assessed after February 12, 2024.
  - For violations occurring on or before November 2, 2015: **$5,500 to $11,000** per violation.

FCA BASICS

The FCA and Cybersecurity

- Cybersecurity is one of DOJ's stated priority areas for FCA enforcement.
- FCA risk related to cybersecurity results from several factors:
  - Complex, agency-specific statutory, regulatory, and contractual provisions.
  - Certification requirements for contractors.
  - Rapidity of information-sharing within the U.S. government related to cyber incidents.
  - Aggressive DOJ theories of FCA fraud, particularly the combined "fraudulent inducement" and "tainted claims" theory.
  - Devotion of significant resources by both DOJ and the relators' bar to investigating and bringing cases.

FCA BASICS

The FCA and Cybersecurity

Cybersecurity Fraud

- Tips for Potential Cybersecurity Whistleblowers
- Generally Applicable Cybersecurity Requirements
- Department of Defense Contractor Cybersecurity Requirements
- GSA Public Buildings Service Contractor Cybersecurity Requirements

Do You Need a Whistleblower Lawyer for Cybersecurity Fraud?

What is cybersecurity fraud?

Cybersecurity fraud is when a government contractor or subcontractor knowingly violates key government requirements to:

i) incorporate specified cybersecurity features when providing goods or services;

ii) take specified measures to protect electronic documents or data; or,

iii) promptly report cybersecurity breaches.

If you know of cybersecurity violations that expose the Government to undue security risk, your information may form the basis for a strong qui tam action.

Shocked, Devastated, Stuck: Cybersecurity Pros Open Up About Their Layoffs

Here's a dose of reality from those on the frontlines and how they're coping.

https://www.informationweek.com/cyber-resilience/shocked-devastated-stuck-cybersecurity-pros-open-up-about-their-layoffs

THE FALSE CLAIMS ACT
RECENT LEGAL DEVELOPMENTS

FCA Impacts from *Chevron* Doctrine's Demise

- FCA cases often hinge on questions of statutory interpretation. For example:
  - Stark Law and Anti-Kickback Statute exceptions / safe harbors established by statute and interpreted via HHS regulations.
  - Medicaid rebate requirements established by statute and interpreted via HHS "best price" regulations.
- In the United States Supreme Court's 1984 ruling in ***Chevron U.S.A. v. Natural Resources Defense Council***, U.S. federal courts were instructed to defer to agencies' interpretations of the laws or statutes they administered.
- The Supreme Court's 2024 decision in ***Loper Bright Enterprises v. Raimondo***, overruled *Chevron*, holding that courts must independently interpret agency statutes without deference to agency readings of those statutes.

Citations: Chevron U.S.A. v. Natural Resources Defense Council, 467 U.S. 837 (1984); *Loper Bright Enterprises v. Raimondo*, 144 S. Ct. 2244 (2024)

FCA Impacts from *Chevron* Doctrine's Demise

- We are already seeing courts grapple with *Loper Bright* in the FCA context, inserting court interpretations of foundational statutory provisions where they previously would have accorded deference to agency interpretation.
  - Most notably, in ***United States ex rel. Sheldon v. Forest Labs., LLC***, 2024 WL 3555116 (D. Md. July 23, 2024), the district court granted the defendant's motion to dismiss, holding that the relator had not adequately pled falsity or scienter. In doing so, the court independently interpreted the Medicaid Drug Rebate Statute, 42 U.S.C. § 1396r-8, expressly stating that it was not relying on CMS's interpretation of that statute, as required by *Loper Bright*.

Supreme Court Precedent on FCA Scienter

- In its 2023 opinion in ***United States ex rel. Schutte v. SuperValu Inc.***, the U.S. Supreme Court unanimously held that FCA scienter turns on a defendant's subjective knowledge at the time of the relevant conduct.
  - Before *SuperValu*, some lower courts had permitted defendants to defend against FCA scienter obligations with objectively reasonable interpretations of ambiguous legal requirements from which the defendants were not "warned away" by existing legal authority.
  - Other courts had rejected this approach, concluding that it prioritized post-hoc litigation positions over contemporaneous facts.
  - *SuperValu* put this debate to rest by holding that an FCA defendant can vitiate scienter by putting the ambiguity of a particular legal requirement at issue, but only with evidence of contemporaneous subjective belief in a particular interpretation of the requirement—not with post-hoc arguments.
- *SuperValu* established a limit on FCA defendants' ability to put interpretations of ambiguous statutes at issue. *Loper Bright* may fill part of that gap by making agency interpretations fair game in litigation regardless of what a defendant thought at the time of its conduct.

THE FALSE CLAIMS ACT ENFORCEMENT PRIORITIES AND TRENDS

DOJ's Civil Cyber-Fraud Initiative

- On October 6, 2021, Deputy Attorney General ("DAG") Lisa O. Monaco announced the launch of DOJ's Civil Cyber-Fraud Initiative, combining DOJ's civil fraud enforcement, government procurement and cybersecurity expertise "to combat new and emerging cyber threats to the security of sensitive information and critical systems."
- The Civil Cyber-Fraud initiative uses the FCA to pursue cybersecurity-related fraud by government contractors and grant recipients that are "***knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches***."
- Whereas earlier cybersecurity FCA enforcement was initiated primarily by *qui tam* relators, the announcement reflects the Biden Administration's increasing emphasis on affirmatively policing cybersecurity requirements for government contractors and their suppliers.

"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward to report it."

-DAG Lisa Monaco

DOJ's Civil Cyber-Fraud Initiative

- On October 13, 2021, the Principal Deputy Assistant Attorney General ("PDAAG") for DOJ's Civil Division, Brian Boynton, delivered remarks on this new initiative, noting the Civil Cyber Fraud Initiative "***will use the [FCA] to identify, pursue and deter cyber vulnerabilities and incidents that arise with government contracts and grants and that put sensitive information and critical government systems at risk***."
- In his speech, calling the FCA "a natural fit to pursue knowing failures" to comply with contracting requirements, PDAAG Boynton identified "three common cybersecurity failures" that would be "prime candidates" for potential FCA enforcement by DOJ:
  - **"knowing failures to comply with cybersecurity standards" in government contracts;**
    - *Example*: The government purchases hardware or software with cyber requirements, and the requirements are not met.
    - *Example:* A contractor implements IT systems for the government and does not comply with contract requirements, including U.S. citizenship requirements.
  - **"knowing misrepresentation of security controls and practices"; and**
    - *Example:* A contractor has an IT system that houses government data, and cyber requirements applicable to that system or data are not met.
    - *Example:* A contractor is providing cloud services, i.e., through FedRAMP, and requirements are not met.
  - **"knowing failure to timely report suspected breaches."**

DOJ's Cooperation Credit Policy

- In May 2019, DOJ issued a policy regarding the circumstances under which it would award cooperation credit in FCA cases.
- For several years thereafter, DOJ's settlement agreements did not explcitly discuss cooperation credit, and DOJ's application of the policy in specific cases thus went unexplained to the public.
- A recent cybersecurity-related FCA resolution heralds greater transparency but leaves some questions unanswered:
  - On **September 5, 2023**, DOJ settled allegations that **Verizon Business Network Services LLC** violated the FCA by failing to implement required cybersecurity controls in connection with GSA contracts for the provision of internet protocol service.
  - DOJ's press release highlighted the company's self-disclosure, and while the settlement agreement identified other forms of cooperation Verizon undertook, it did not specify which factors, if any, carried more weight than others in the credit determination.
  - The total settlement amount was approximately 1.5 times the alleged single damages—a multiplier higher than what DOJ has agreed to elsewhere without self-disclosure.

2024 DOJ FCA Enforcement Priorities

DOJ's FCA enforcement priorities for 2024, as stated by PDAAG Boynton at a February 2024 conference, are as follows:

(1) Cybersecurity fraud

(2) COVID-19 pandemic fraud

(3) Healthcare fraud, specifically illegal inducements and schemes involving nursing homes (echoing DOJ's stated focus on elder fraud more broadly)

(4) Accountability for third parties that cause the submission of false claims, including private equity firms

"We continue to encourage companies to take advantage of the government's False Claims Act cooperation policy. It offers companies an opportunity to mitigate their potential liability. It is also the right thing to do for our security."

- PDAAG Brian Boynton

ENFORCEMENT PRIORITIES & TRENDS

General Enforcement Trends

➢ ***FY2023***:

- FY2023 was a record-breaking year in terms of new FCA cases.
- There were **1,212 new cases**—a 26% increase over FY2022 (the prior record).
- **500 of these were cases initiated by the government** based on referrals or investigations (rather than *qui tam* matters)—breaking a record (340) last set in 1987.
- The government obtained approximately **$2.7 billion** in FCA recoveries from settlements and judgments. **$550 million** of these were in the defense industry alone.
- By comparison, FY2022 saw approximately **$2.2 billion** in FCA recoveries.

➢ ***First half of calendar year 2024***:

- Through June 30, 2024, the government entered into resolutions totaling **over $1 billion** in recoveries—the highest in recent memory for the first half of a year.
  - Two of these settlements had face values each in the **hundreds of millions**.
- There was also a jury verdict of **approximately $150 million** in mid-June, in a case in which DOJ **declined to intervene**.
- Recoveries in the health care and life sciences industries continue to dominate enforcement activity, but the first half of 2024 witnessed four FCA settlements with government contractors with values each in the eight figures.

GOVERNMENT CONTRACTING

CONTRACTOR CYBERSECURITY: OVERVIEW & CYBER INCIDENT REPORTING

CONTRACTOR CYBERSECURITY: OVERVIEW

"Safeguarding" Clauses

- **FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems**
  - "The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. . . ."
  - Applies to every federal contract, except for acquisitions of commercially available off-the-shelf (COTS) items, "when a contractor's information system may contain Federal contract information" (FCI) – FAR 4.1902
- **DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**
  - "The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections . . . ."
  - Applies to all DoD "solicitations and contracts," except for COTS items – DFARS 204.7304
  - Compliance with NIST 800-171

FedRAMP

- Federal Risk and Authorization Management Program (FedRAMP) was established in 2011 to safely accelerate the adoption of commercial cloud computing products and services by Federal agencies, focusing on a consistent, reusable approach to security assessments and authorizations.
  - FedRAMP has been historically focused on securely facilitating federal agencies' use of commercially available infrastructure as a service (IaaS) offerings, but in recent years there has been increased focus on the area of software as a service (SaaS).
- When a Cloud Service Offering (CSO) meets the rigorous security standards and authorization requirements, it is considered FedRAMP-authorized, and presumed to have adequate security for use by federal agencies.
- Defining the authorization boundary is one of the more complicated and critical tasks to ensure compliance and avoid potential liability, including under the False Claims Act.
  - Under OMB A-130, the authorization boundary includes "all components of an information system to be authorized for operation…"

CYBER INCIDENT REPORTING

Cyber Incident Reporting – Government Contracts (FAR / DFARS)

- Contractors may be subject to contractual requirements that they report breaches of contractor information systems to the government or to prime contractors (or higher-tier subcontractors).
- Cyber incident clauses may be tailored to individual contracts/agreements.
  - E.g., a contract with DOD made pursuant to the agency's Other Transaction Authority, which will not incorporate clauses from the FAR or DFARS.
- **DFARS 252.204-7012**, Safeguarding Covered Defense Information and Cyber Incident Reporting, is incorporated into all DOD solicitations and contracts (except for COTS).
  - "When the contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract," the Contractor is required to rapidly report.
  - "**Rapidly report** " means "within **72 hours** of discovery of any cyber incident" – DFARS 252.204-7012(a).

CYBER INCIDENT REPORTING

Cyber Incident Reporting – DFARS 252.204-7012

- Reports of cyber incidents must be made via DIBNet.
- DIBNet serves both as a centralized portal for reporting by companies, and as a tool to facilitate rapid information-sharing within DOD and beyond.
- This means that companies holding contracts with multiple DOD agencies, and with agencies outside DOD, must have robust mechanisms for responding to rapid follow-up from government agencies in response to a cyber incident report.
- This puts a premium on clear processes for internal coordination between legal, contract managers, business units involved in specific contracts, and cybersecurity subject-matter experts.

CYBER INCIDENT REPORTING

Cyber Incident Reporting Under FedRAMP

- On September 12, 2024, FedRAMP updated its Incident Communications Procedures.
- The procedures require Cloud Service Providers to report suspected and confirmed security incidents within 1 hour of identification.
- Reports must be made to customers affected or suspected of being affected, as well as to FedRAMP, agency authorizing officials, and—depending on the attack vector—the Cybersecurity and Infrastructure Security Agency (CISA).

ONGOING DEVELOPMENTS

Cybersecurity Maturity Model Certification (CMMC)

- DOD introduced CMMC 1.0 in January 2020, as a tiered framework for cybersecurity requirements for members of the Defense Industrial Base (DIB).
- CMMC 2.0 was introduced in November 2021, purportedly as a "simplified" version of CMMC 1.0.
  - But CMMC 2.0 proved still quite complex, and application to contractors continued to be left to the rulemaking process.
- On August 14, 2024, DOD published a proposed rule that would implement CMMC 2.0 in the contracting process, in particular by specifying the CMMC level required by a solicitation and the CMMC certificate or self-assessment results that must be posted prior to contract award.

HEALTH CARE AND CYBERSECURITY

CYBERSECURITY RISKS FOR DEVICE MANUFACTURERS

Cybersecurity Risks for Medical Devices

- Certain medical devices carry cybersecurity risks:
  - In August 2017, the FDA recalled almost 500,000 pacemakers because they were potentially vulnerable to hacking.
  - The 2017 “Wannacry” ransomware attack affected devices such as MRI scanners in UK hospitals.
- The Food, Drug, and Cosmetic Act (FDCA) was amended in December 2022 to require that premarket submissions to the FDA for approval of cyber devices contain cybersecurity information.
- Required information includes plans to address cybersecurity vulnerabilities; processes to provide reasonable assurances that devices are cybersecure; and a software bill of materials.

Amendments to the Food, Drug, and Cosmetic Act (FDCA)

- These amendments create FCA risks in the form of a "fraud-on-the-FDA" theory of liability, under which a misrepresentation to the FDA in the device approval process renders subsequent claims for payment for the device (e.g., by Medicare and Medicaid) false under the FCA.
  - The theory is controversial:
    - The First Circuit rejected it due to lack of a causal link between representations to the FDA, on the one hand, and payments by CMS, on the other hand. (*D'Agostino v. EV3, Inc.*, 2016)
    - Subsequently, the Ninth Circuit let two cases proceed on the basis of the theory. (*Dan Abrams Co. v. Medtronic, Inc.*, 2021; *U.S. ex rel. Campie v. Gilead Scis., Inc.*, 2017)

FALSE CLAIMS ACT CYBERSECURITY DEVELOPMENTS

CYBERSECURITY DEVELOPMENTS – KEY TAKEAWAYS

Focus on Cybersecurity – Key Takeaways

- DOJ's focus on cybersecurity, via the Civil Cyber-Fraud Initiative, has been marked by an increasing number of FCA settlements and the first-ever DOJ intervention in a cybersecurity-related FCA case—with another intervention possible in the near future.
- The cybersecurity-related settlements involve both the defense sector and other industries, including healthcare contractors; and involve both direct federal contracts and state projects supported by federal funds.
- The dollar values of the settlements are lower than those of many FCA settlements in other areas, but larger recoveries can be anticipated given DOJ's commitment of resources to cybersecurity enforcement.
- The intervened lawsuit is against a university, as is the case in which DOJ continues to assess whether to intervene.
  - The intervened case alleges fraudulent misrepresentations of compliance with requirements to safeguard sensitive DOD information.
  - The complaint focuses on two DOD contracts worth approximately $31.2 million, suggesting a potential recovery far in excess of prior FCA cybersecurity resolutions.

RECENT ENFORCEMENT ACTIONS

Focus on Cybersecurity – Settlements

- Comprehensive Health Services, Inc.: In March 2022, Comprehensive Health Services paid $930,000 to resolve allegations that it misrepresented its compliance with State Department contract requirements to store medical records in a secure EMR system.
  - Contract clause at issue: FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
- Aerojet Rocketdyne, Inc.: In July 2022, defense- and space-sector contractor Aerojet paid $9 million to resolve allegations that it misrepresented its compliance with DOD regulations to safeguard controlled unclassified information (CUI), and with a NASA rule for protecting sensitive information.
  - Contract clauses at issue:
    - DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
    - NFS 1852.204-76, Security Requirements for Unclassified Information Technology Resources

RECENT ENFORCEMENT ACTIONS

Focus on Cybersecurity – Settlements

- Jelly Bean Communications Designs LLC (Jelly Bean): In March 2023, Jelly Bean agreed to pay approximately $300,000 to resolve allegations that it violated the FCA by failing to secure personal information on a federally funded Florida children's health insurance website, which Jelly Bean created, hosted, and maintained. DOJ claimed that, contrary to its representations in agreements and invoices, Jelly Bean knowingly failed to maintain, patch, and update the website's software systems, leaving the site vulnerable to attack.
  - Contract clause at issue: requirement for provision of HIPAA-compliant hosting environment
- Verizon Business Network Services LLC: In September 2023, Verizon agreed to pay approximately $4 million to resolve FCA allegations regarding failure to satisfy cybersecurity controls required under certain General Services Administration (GSA) contracts.
  - Contract clauses at issue: clauses requiring compliance with Critical Capabilities specified in DHS TIC Reference Architecture

RECENT ENFORCEMENT ACTIONS

Focus on Cybersecurity – Settlements

- Insight Global LLC: In May 2024, Insight Global agreed to pay approximately $2.7 million to resolve allegations that it violated the FCA by failing to implement adequate cybersecurity measures in connection with personal health information obtained during COVID-19 contact tracing procedures the company performed for the Pennsylvania Department of Health.
  - Contract clause at issue: clause requiring that personal health information be "kept confidential and secure"
- Guidehouse Inc. / Nan McKay & Associates: In June 2024, these two companies agreed to pay a combined $11.3 million to resolve FCA allegations stemming from cybersecurity requirements in contracts to provide an online application for the federal emergency rental assistance program established in early 2021. DOJ alleged that the companies failed to conduct required cybersecurity testing before the online application went live, and that a security breach was identified 12 hours after the application went online.
  - Contract clauses at issue: requirements for pre-launch cybersecurity testing and scanning

RECENT ENFORCEMENT ACTIONS

Focus on Cybersecurity – Lawsuits

Georgia Institute of Technology

- February 2024: DOJ intervened in a *qui tam* lawsuit, originally filed in July 2022, alleging that Georgia Institute of Technology, Georgia Tech Research Corporation, and Georgia Tech Research Institute failed to comply with NIST 800-171 mandatory cybersecurity controls in their DOD contracts, thus failing to comply with DFARS 252.204-7012.
- The complaint alleges that Georgia Tech made false statements regarding its compliance with this provision, thereby fraudulently inducing DOD to enter into two contracts worth approximately $31.2 million.
- The suit was brought by the Associate Director of Cybersecurity at Georgia Tech and the Principal Information Security Engineer.
- In August 2024, DOJ filed its complaint-in-intervention.
- This is the first FCA case of its kind in which DOJ has intervened.

Focus on Cybersecurity – Lawsuits

Georgia Institute of Technology (cont'd)

- Allegations in DOJ's complaint:
  - Defendants allegedly failed to (i) implement a compliant System Security Plan, (ii) use antivirus software on devices that had access to nonpublic DOD information, and (iii) submit an accurate summary score of NIST 800-171 guidance.
  - As part of their failure to implement a compliant System Security Plan, Defendants allegedly omitted most of the relevant lab's computers (endpoints) from the scope of the plan.
  - Defendants allegedly provided a false cybersecurity compliance score based on a non-existent campus-wide IT system, despite a former employee warning them that doing so would be misleading to DOD.
  - The government allegedly got little or no value from the technology that Defendants provided, because what DOD bargained for was for its military technology to be stored in a secure environment, which Defendants failed to provide.
  - Georgia Tech personnel allegedly knew the university was noncompliant and was at risk of FCA liability.
- The relators were both university insiders with access to relevant information.

Focus on Cybersecurity – Lawsuits

Georgia Institute of Technology (cont'd)

- Implications for contractors:
  - Given DOJ's focus on the alleged fraudulent inducement of contracts to which Georgia Tech was not entitled, the case highlights the importance of early vetting of award submissions, in addition to go-forward checks over the course of contract performance.
  - The complaint also alleges that Georgia Tech's compliance culture gave undue power to university researchers who brought in contracting money, thus highlighting the importance of an independent compliance function, compliance training tailored to different roles and functions, and strong mechanisms for internal reporting and investigation.
  - Highlights the importance of legal and IT/cybersecurity teams working together and ensuring consistent understanding of contractual obligations.

One Embarcadero Center, Suite 2600, San Francisco, CA 94111-3715

+1 415.393.8362

wchan@gibsondunn.com

Winston Y. Chan

Partner / San Francisco

Winston Y. Chan is a litigation partner in Gibson, Dunn & Crutcher's San Francisco office, and serves as co-chair of the firm's White Collar Defense and Investigations practice group, and also its False Claims Act/Qui Tam Defense practice group. He leads matters involving government enforcement defense, internal investigations and compliance counseling, and regularly represents clients before and in litigation against federal, state and local agencies, including the U.S. Department of Justice, Securities and Exchange Commission and State Attorneys General. His investigations experience also includes hundreds of witness interviews in Mandarin Chinese in the life sciences, healthcare, hospitality, consumer products, and information technology industries.

Winston is a *Chambers*-ranked attorney in the category of White Collar Crime and Government Investigations, and *Benchmark Litigation* recognizes him as a Litigation Star for being "recommended consistently as a reputable and effective litigator by clients and peers." He is regularly included in *Best Lawyers*, *The Legal 500*, and *Who's Who Legal* for Investigations.

Prior to joining the firm, Winston served as an Assistant United States Attorney in the Eastern District of New York, where he investigated a wide range of corporate and financial criminal matters as part of that office's Business and Securities Fraud Section. Winston additionally prosecuted cases in the Organized Crime and Racketeering Section, where he handled matters involving Italian, Eastern European and Asian criminal enterprises, for which the Attorney General awarded Winston one of the Department of Justice's highest awards for his "exemplary and historic work." As a senior prosecutor, Winston served in a number of supervisory roles at the U.S. Attorney's Office, including as Deputy Chief of the General Crimes section, where he supervised and trained that office's line prosecutors, as well as Health Care Fraud Coordinator, where he oversaw criminal healthcare fraud and qui tam matters.

Winston earned his undergraduate degree, *magna cum laude*, from Yale University, and his Juris Doctor from Yale Law School, where he was on the *Yale Law Journal* and president of the Pacific Islander, Asian and Native American Law Students' Association. Following law school, Winston served as a law clerk for the Honorable Leonard B. Sand of the United States District Court for the Southern District of New York, and then for the Honorable Chester J. Straub of the United States Court of Appeals for the Second Circuit. While a federal prosecutor, Winston taught a clinical course at Columbia Law School on the principles of federal prosecution and a first-year lawyering course at Fordham University School of Law.

Winston's full biography can be viewed here.

EDUCATION

Yale University
Juris Doctor

Yale University
Bachelor of Arts, *magna cum laude*

CLERKSHIPS

U.S. Court of Appeals, 2nd Circuit

U.S.D.C., Southern District of New York

EDUCATION

Stanford University
Juris Doctor

U.S. Naval Academy
Bachelor of Science

Georgetown University
Master of Arts

GIBSON DUNN

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.955.8510

shandler@gibsondunn.com

Stephenie Gosnell Handler

Partner / Washington, D.C.

Stephenie Gosnell Handler is a partner in Gibson Dunn's Washington, D.C. office, where she is a member of the International Trade and Privacy, Cybersecurity, and Data Innovation practices. She advises clients on complex legal, regulatory, and compliance issues relating to international trade, cybersecurity, and technology matters. Stephenie 's legal advice is deeply informed by her operational cybersecurity and in-house legal experience at McKinsey & Company, and also by her active duty service in the U.S. Marine Corps.

Stephenie returned to Gibson Dunn as a partner of the Washington, D.C. office after serving as Director of Cybersecurity Strategy and Digital Acceleration at McKinsey & Company. In this role, she led development of the firm's cybersecurity strategy and advised senior leadership on public policy and geopolitical trends relating to cybersecurity, technology, and data. Stephenie managed a team of experienced professionals responsible for the firm's cybersecurity strategic initiatives, cybersecurity standards and certifications program, lifecycle governance initiatives, data analytics and optimization, and digital acceleration efforts across the cyber domain. She previously led McKinsey's in-house cybersecurity legal team, where she advised on diverse global cybersecurity and technology matters, including strategic legal issues, data localization, regulatory compliance, risk management, governance, preparedness, and response. Stephenie frequently advised at the intersection of cybersecurity, technology, and data and export control and sanctions requirements.

Previously, Stephenie was a senior associate at a leading international law firm, where she focused her practice on international trade matters including CFIUS, export controls, and sanctions, and cybersecurity matters across the cybersecurity risk management and incident lifecycle, including assessments, incident response preparedness, incident response, regulatory compliance, transactional due diligence, and regulatory enforcement actions.

Stephenie started her legal career at Gibson Dunn, where she focused on international trade, cybersecurity, and transactional matters.

Stephenie earned her J.D. from Stanford University in 2011. She earned her M.A. from Georgetown University and her B.S. from the U.S. Naval Academy, both in 2001. Prior to attending law school, Stephenie served as officer in the U.S. Marine Corps, where she focused on logistics and political-military affairs during her seven years of active duty service.

Stephenie's full biography can be viewed here.

1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.887.3579

mfarrar@gibsondunn.com

Melissa L. Farrar

Partner / Washington, D.C.

Melissa Farrar is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher. Her practice focuses on white collar defense, internal investigations, and corporate compliance. Most recently, Melissa was recognized by the 2024 edition of *Best Lawyers: Ones to Watch® in America* for Criminal Defense: White-Collar.

Melissa represents and advises multinational corporations in internal and government investigations on a wide range of topics, including the U.S. Foreign Corrupt Practices Act, the False Claims Act, anti-money laundering, and accounting and securities fraud, including defending U.S. and global companies in civil and criminal investigations pursued by the U.S. Department of Justice ("DOJ") and the U.S. Securities and Exchange Commission ("SEC"). She also has experience representing U.S. government contractors in related suspension and debarment proceedings.

Her defense and investigations work has included successful representation of companies across a variety of industries, including those in the pharmaceutical, telecommunications, technology and software-as-a-service ("SaaS"), manufacturing, consumer products, rail transportation, oil and gas, and defense spaces, among others.

Melissa also routinely counsels corporations in these and other industries on the design and implementation of their corporate ethics and compliance programs and in connection with transactional due diligence, with a particular emphasis on compliance with anti-corruption and anti-money laundering laws. She frequently leads corporate compliance program assessments and has experience in all areas of corporate compliance, including policy and procedure and code of conduct development, program governance and structure design, risk assessment planning and implementation, and the conduct of internal investigations, among others.

She was named by Expert Guides in its 2021 and 2022 *Rising Stars Guide*, which recognizes the brightest and most talented practitioners under 40 in the area of business law and related practices.

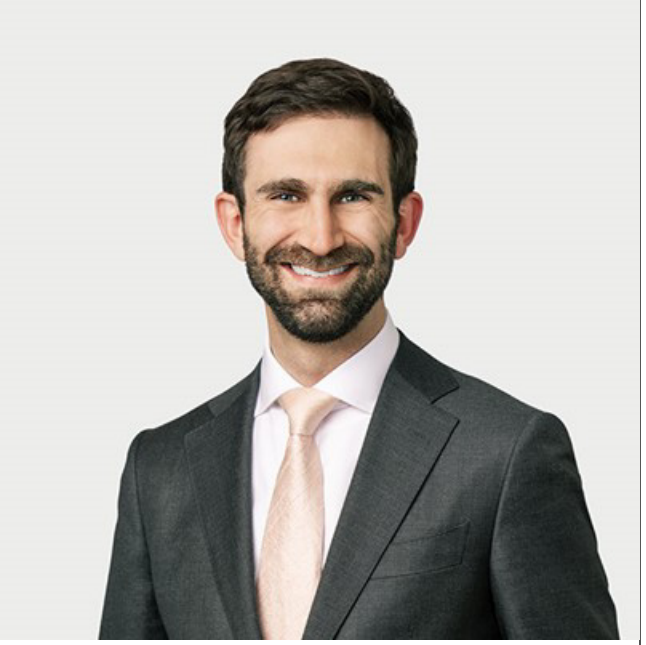
Melissa received her law degree with high honors from the George Washington University Law School in 2013, where she was elected to the Order of the Coif. While in law school, she was a member of the George Washington Law Review. She received her Bachelor of Arts degree in 2004 from Dartmouth College.

Melissa's full biography can be viewed here.

EDUCATION

George Washington University
Juris Doctor

Dartmouth College
Bachelor of Arts



1700 M Street, N.W., Washington, D.C. 20036-4504

+1 202.955.8252

mdziuban@gibsondunn.com

Michael R. Dziuban

Associate / Washington, D.C.

Michael R. Dziuban is a senior associate in the Washington, D.C. office of Gibson, Dunn & Crutcher, where he practices in the firm's litigation department. Michael represents and counsels clients in white collar defense and civil enforcement matters, including investigations and lawsuits under the False Claims Act and related state laws. He has advised health care companies, government contractors, technology companies, and individual executives in various stages of False Claims Act enforcement opposite both government agencies and *qui tam* relators. Michael has particular experience handling False Claims Act matters for clients who participate in federal healthcare programs, including matters involving allegations of the Anti-Kickback Statute and requirements related to coverage for prescription drugs. Michael also regularly counsels clients on corporate compliance matters related to the health care fraud and abuse laws.

As part of his broader practice, Michael has guided clients through government and internal investigations under anti-corruption and anti-money laundering laws, advised clients in government contracts disputes, and counseled companies on their corporate compliance programs. Michael also has dedicated significant time to pro bono criminal defense work while at Gibson Dunn, serving on two teams that each won the firm's Frank Wheat Memorial Award. One of those matters culminated in the release of Gibson Dunn's client after 20 years of wrongful imprisonment.

Michael received his law degree *cum laude* from Harvard Law School in 2015. Between college and law school, he worked in the Middle East Program at the Center for Strategic and International Studies in Washington, D.C., where he researched and wrote on U.S. policy in the Middle East.

Michael is admitted to practice in the District of Columbia and the Commonwealth of Virginia.

Michael's full biography can be viewed here.

EDUCATION

Harvard University
Juris Doctor

Yale University
Bachelor of Arts

Upcoming Programs – Fall White Collar Webcast Series

Date and Time	Program	Registration Link
Thursday, September 26, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT 6:00 PM – 7:00 PM CET	**Running Internal Investigations Effectively** Presenters: Benno Schwarz, Katharina Humphrey, Oleh Vretsona	Event Details
Tuesday, October 1, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT	**DOJ's Consumer Protection Branch** Presenters: Nicola Hanna, Gustav Eyler, Katlin McKelvie	Event Details
Wednesday, October 2, 2024 12:00 PM – 1:00 PM ET 9:00 AM – 10:00 AM PT	**Navigating Parallel Investigations: Managing Simultaneous DOJ and SEC Investigations** Presenters: Douglas Fuchs, Poonam Kumar, Mark Schonfeld	Event Details

THANK YOU!

Please note that the enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.