GIBSON DUNN

Webcast: False Claims Act Enforcement Developments and Trends – Cybersecurity

Webcasts | September 24, 2024

The False Claims Act (FCA) is one of the most powerful tools in the government's arsenal to combat fraud, waste, and abuse involving government funds. Nearly three years ago, the Department of Justice announced the establishment of the Civil Cyber-Fraud Initiative to utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients. Since the announcement of the Civil Cyber-Fraud Initiative, the government has continued to promulgate new cybersecurity requirements and reporting obligations in government contracts and funding agreements—which may bring yet more vigorous FCA enforcement efforts by the DOJ. The DOJ, moreover, has entered into several notable FCA settlements premised on alleged cybersecurity violations, and has intervened in a first-of-its kind qui tam case related to DoD cybersecurity regulations. As we approach the third anniversary of the launch of the Civil Cyber-Fraud Initiative, as much as ever, companies that receive government funds—especially companies operating in the government contracting sector—need to understand how the government and private whistleblowers alike are wielding the FCA to enforce required cybersecurity standards, and how they can defend themselves. Please join this recorded webcast which discusses developments in the FCA, including:

- The latest trends in FCA enforcement actions and associated litigation affecting government contractors, including technology companies;
- Updates on enforcement actions arising under the DOJ Civil Cyber-Fraud Initiative;
- The latest trends in FCA jurisprudence, including developments in particular FCA legal theories affecting your cybersecurity compliance and reporting obligations; and
- Updates to the cybersecurity regulations and contractual obligations underlying enforcement actions by DOJ's Civil Cyber-Fraud Initiative.

PANELISTS: Winston Y. Chan is a partner in the San Francisco office of Gibson Dunn and 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. Winston is admitted to practice law in the state of California. **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.

Related People

Winston Y. Chan

Stephenie Gosnell Handler

Melissa L. Farrar

Michael R. Dziuban

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. **Melissa L. 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. 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 and the U.S. Securities and Exchange Commission. She also has experience representing U.S. government contractors in related suspension and debarment proceedings. In addition, Melissa routinely counsels corporations 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 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. Melissa is admitted to practice in the District of Columbia and Virginia. **Michael R. Dziuban** is a senior associate in the Washington, D.C. office, where he practices in the Firm's Litigation Department. 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, healthcare 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. Michael is admitted to practice law in the Commonwealth of Virginia and the District of Columbia.

MCLE CREDIT INFORMATION: This program has been approved for credit in accordance with the requirements of the New York State Continuing Legal Education Board for a maximum of 1.0 credit hour, of which 1.0 credit hour may be applied toward the areas of professional practice requirement. This course is approved for transitional/non-transitional credit. Attorneys seeking New York credit must obtain an Affirmation Form prior to watching the archived version of this webcast. Please contact CLE@gibsondunn.com to request the MCLE form. Gibson, Dunn & Crutcher LLP certifies that this activity has been approved for MCLE credit by the State Bar of California in the amount of 1.0 hour in the General Category. California attorneys may claim "self-study" credit for viewing the archived version of this webcast. No certificate of attendance is required for California "self-study" credit.

GIBSON DUNN

Related Capabilities

False Claims Act / Qui Tam Defense

White Collar Defense and Investigations