Preparing for the DOJ'S NEW CIVIL CYBER-FRAUD INITIATIVE

On October 6, 2021, the US Department of Justice (DOJ) announced the Civil Cyber-Fraud Initiative "to combat new and emerging cyber threats to the security of sensitive information and critical systems."[1] The Commercial Litigation Branch's Fraud Section of the Civil Division leads the Initiative along with civil enforcement attorneys in each of the 94 US Attorney Offices, the Inspector General Offices, and other agencies.

The Initiative "combine(s) the department's expertise in civil fraud enforcement, government procurement and cybersecurity" to target government contractors and recipients of federal funds who fail to comply with cybersecurity standards. Deputy Attorney General Lisa O. Monaco, the second-highest ranking DOJ officer, stated that DOJ government contractors and grant recipients "entrusted to work on sensitive government systems" who "fail to follow required cybersecurity standards" will be subject to "**very hefty fines**" under the Initiative.[2]

This Initiative, bringing dedicated civil enforcement resources to bear on a specific type of conduct, will spawn both False Claims Act (FCA) investigations and litigation initiated by both the DOJ and qui tam relators. The Initiative is part of a broader focus by the Biden administration on cybersecurity issues,[3] and is a product of the DOJ Comprehensive Cyber Review.[4]

Q1. What Types of Conduct Will the Initiative Be Targeting?

- According to the DOJ announcement, the Initiative intends to focus on corporate and individual conduct that places federal government information or systems at risk by:

[1] *See* Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021).
[2] *See* Eric Tucker, US poised to sue contractors who don't report cyber breaches, AP News (Oct. 6, 2021) (emphasis added).
[3] *See* Executive Order on Improving the Nation's Cybersecurity (May 12, 2021).
[4] *See* Remarks of Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A. Polite, Jr. at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape,' (Oct. 20, 2021) (discussing Comprehensive Cyber Review).

- Knowingly providing **deficient cybersecurity products or services**,
- Knowingly **misrepresenting cybersecurity practices or protocols**, or
- Knowingly **violating obligations to monitor and report** cybersecurity incidents and breaches.

- While these broad categories of conduct reach a wide range of activities, the group leading the Initiative can be expected to consider within its "jurisdiction" all manner of cybersecurity noncompliance by contractors and subcontractors that adversely affect federal programs.
- The Initiative also will "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."[5]

Q2. When a CyberAttack or Cyber Incident Occurs, What Steps Should Be Taken as Part of a Cyber Investigation?

- There are many cyber risks that may impact or disrupt a company or organization, most involving cybercrime. The risks comprise phishing schemes, business email compromise or fraud schemes, email account takeover cases, ransomware, targeted cyberattacks, and incidents involving third-party vendors possessing government information or another company's data, to name a few.

- To determine the scope and timing of the cyber incident, a **cyber investigation** should be conducted, typically at the direction of counsel to **preserve the attorney-client privilege and any attorney work product** on behalf of the company. Data should be preserved and collected in a forensically sound manner. Depending on the nature of the incident and potential risk, the Law Department should be alerted to determine the manner of the cyber investigation, the scope of privileged issues, and whether experienced counsel and forensic specialists should be engaged.

- The cyber investigation normally will involve a forensic specialist engaged and working at the direction of counsel to determine whether any data was accessed, acquired, or exfiltrated and the scope of the incident. Depending on the forensic facts, notifications may be required to be sent to government agencies, federal and state regulators, other companies, and individuals.

- The **manner in which the cyber incident is investigated and responded to** may impact business relations, federal and state regulatory investigations and enforcement, litigation risk, and FCA liability. Experienced cyber counsel can assist with all phases in a cyber investigation.

- **Key phases in a cyber investigation** typically include:
  a) Preparation in advance including an Incident Response Plan;
  b) Detection of the cyber incident;
  c) Conducting the cyber investigation, assessment, and analysis;
  d) Containing and eradicating the cyber threat and restoring security;
  e) Remediation and recovery;

[5] *See* Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit, Washington, DC (Oct. 13, 2021).

f) Determining whether and when to submit a report to law enforcement and which agency is appropriate, and working with law enforcement;
g) Determining and managing notifications to government agencies, federal and state regulators, individuals, and business partners;
h) Addressing legal issues such as FCA questions or whether a "breach" occurred depending on applicable federal, state, or contractual standards;
i) Considering public statements and addressing reputational issues;
j) Maintaining and addressing business relations;
k) Anticipating and being prepared for regulatory inquiries and investigations; and
l) Anticipating and being prepared for potential civil litigation.

Q3. What Is the False Claims Act?

- The FCA, 31 U.S.C. §§ 3729-3733, is the government's principal civil fraud enforcement tool.
- The FCA, a Civil War–era statute, imposes liability on companies and individuals who defraud the government of money or property.
    - In general, liability arises based on knowingly submitting or causing to be submitted to the government a false or fraudulent claim for payment, or knowingly avoiding an obligation to pay money to the government.
    - The FCA reaches "knowing" conduct by companies and individuals, which includes specific intent as well as lesser levels of scienter, namely reckless disregard and deliberate ignorance.
- A unique feature of the FCA is its qui tam provision, which empowers private parties to pursue civil suits based on FCA violations on behalf of the government and to receive a percentage share of any resulting recovery by judgment or settlement.

Q4. What Type of Penalties and Remedies Does the FCA Provide?

- Upon a finding of liability, an FCA defendant is liable for **treble the amount of damages** sustained by the government due to the FCA violation.
- In addition, the court must impose per-claim penalties of up to $23,331, which can result in tens of millions of dollars in penalties (even when actual damages are low) where hundreds or thousands of claims are involved.
- Over the last several years, annual recoveries in FCA cases have ranged from $2 billion to **$5 billion**.
- Although not specified in the FCA itself, a finding of FCA liability (and in some instances allegations alone) can result in **suspension and debarment** of companies and individuals, which would severely impact most government contractors.

Q5. How Will the DOJ Initiate and Investigate Cyber-Fraud Matters?

- As the Initiative will be led by the DOJ's Commercial Litigation Branch, investigations will begin from three principal sources:
    1) Federal agency referrals, either from contracting officials or Inspectors General, based on information that comes to their attention.
    2) Qui tam filings: Federal court qui tam actions now average between 600–700 filings per year and these matters comprise the majority of the Commercial Litigation Branch's FCA docket.
        i. The Initiative will incentivize qui tam relators and their counsel to file suit alleging cyber-related FCA violations, knowing that such filings will be referred to and reviewed by an enforcement team experienced in such matters and looking to pursue them.
    3) Affirmative FCA cases: The DOJ has the ability to—and does—pursue cases on its own, without a relator.
- The DOJ will use a variety of means to investigate these matters:
    - FCA Section 3733 authorizes the use of Civil Investigative Demands (CIDs) to compel production of documents, responses to interrogatories, and depositions either prior to filing an FCA complaint or to investigate allegations filed by relators before deciding whether the government will intervene in such matters. CIDs are "one-way" discovery in FCA cases.
    - Agency subpoenas: The DOJ often works with agency Inspector Generals who issue subpoenas to investigate potential FCA violations.
    - Voluntary compliance: The DOJ may simply request a company to provide it with information without formal process, particularly if the company is cooperating and represented by experienced counsel.

Q6. How Will I Know If the DOJ Is Investigating Potential Cyber-Fraud?

- As most FCA matters are prompted by qui tam filings that are made under seal, the DOJ does not initially notify an enforcement target of the suit.
- Often, the first indicators of an FCA investigation are:
    - Service of a CID or Inspector General subpoena compelling the production of documents or materials. It is important that such matters get elevated immediately to the Law Department and that experienced counsel are engaged at the earliest opportunity.
    - Contact between agents and current or former employees, often outside of work hours. Here, too, it is important that reports of such contacts be made to the Law Department as soon as they are identified.

Q7. How Can a Company Mitigate FCA Risk in the Cyber Arena?

- Monitor and review existing cybersecurity compliance standards and efforts and assess whether adjustments need to be made—or resources shifted—to address potential noncompliance with federal cyber standards and contract requirements.
    - Cybersecurity requirements and standards vary depending on the government contract. Some examples may include:
        - Cybersecurity Maturity Model Certification (CMMC)
        - Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident
        - Federal Acquisition Regulation (FAR) 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
        - National Institute of Standards and Technology (NIST) SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
        - NIST SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations
- Know the most likely scenarios for risk:
    - Representations regarding compliance with cyber standards made in the contract proposal. Material false certifications in the proposal can place the company at risk for FCA liability based on a theory that the company was ineligible for contract award and that all resulting claims for payment are false.
    - Representations and certifications of compliance during contract performance, including statements about testing and updating to meet the latest standards.
- Document compliance including written plans and policies.
- Ensure cyber requirements are flowed down to and met by subcontractors and any third-party vendors.
- Provide an avenue to learn about internal issues and potential whistleblower complaints.
- Ensure that communications with the agency about compliance are well documented and accessible.
- When a report of noncompliance surfaces, assess whether a mandatory disclosure is necessary and whether a voluntary disclosure should be made.
- When personnel raise issues, engage with them and ensure that they do not face retaliation.
- Where appropriate, engage counsel to investigate, assess the government contract compliance risk, assist with any disclosure, and engage with the government attorneys and agents handling any FCA investigation.

Q8. What Are Some Recent Examples of Cases?

- Even before the announcement of the Civil Cyber-Fraud Initiative, the FCA was used in cybersecurity cases.

- One qui tam case alleged that a product did not comply with security requirements and ultimately settled for $8.6 million. The relator received approximately $1.75 million, and the states and DC received approximately $6 million with $2.6 million to the federal government.[6] Another qui tam case was dismissed under the FCA standards.[7] The DOJ's emphasis on cybersecurity cases is expected to increase FCA cases.

Q9. How Can Morgan Lewis Help?

- Morgan Lewis has experience handling all types of cyber incidents and investigations and assisting clients on FCA investigations and cases, in cyber litigation, and in federal and state regulatory investigations. Based on this experience, Morgan Lewis can anticipate key issues at all phases of these types of investigations, cases, and litigation.

- Morgan Lewis has assisted clients with the following:

    - Conducting cyber assessments under attorney-client privilege to identify and remediate compliance issues and to ensure that a reasonable cybersecurity program is in place that satisfies regulatory and other requirements;

    - Implementing policies and training regarding data breaches, including governance and risk assessments, data loss prevention, and third-party vendor management;

    - Designing effective Incident Response Plans tailored to the data and risks of the company and conducting tabletop exercises to measure preparedness for a cyberattack or cyber incident;

    - Managing hundreds of cyber incidents and data breaches (including phishing schemes, Business Email Compromise or fraud account takeover cases, ransomware, targeted cyberattacks, and incidents) and conducting a privileged cyber investigation;

    - Handling numerous investigations and cases involving FCA matters including those involving allegations of noncompliance with cybersecurity standards and contract requirements;

    - In appropriate cases, coordinating with law enforcement and responding to requests;

    - Responding to federal and state agency inquiries and investigations including by the DOJ, SEC, FTC and numerous state attorneys general, including investigations involving overlapping jurisdiction; and

    - Successfully defending data privacy class actions—either winning motions to dismiss or defeating class certifications in lawsuits brought after data breaches or based upon alleged violations of a company's privacy policy.

---

[6] *U.S. ex rel. Glenn v. Cisco Sys.*, No. 1:11-cv-00400 (W.D.N.Y. 2019).

[7] *U.S. ex rel. Adams v. Dell Comput.*, No. 15-cv-608 (D.D.C. 2020) (declined qui tam case alleging sale of computer products with undisclosed cybersecurity hardware vulnerabilities). *See also U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240 (E.D. Cal. 2019) (declined qui tam case brought by insider alleging noncompliance with contractual cybersecurity requirements).

PRESENTERS / CONTACTS

Mark L. Krotoski
Silicon Valley | Washington, DC
+1.650.843.7212 | +1.202.739.5024
mark.krotoski@morganlewis.com

- Co-Head of the Privacy and Cybersecurity Practice and Litigation Partner
- Former DOJ cybercrime prosecutor and National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division, prosecuting and investigating all forms of domestic and international cyberattacks and cybercrimes.

Douglas W. Baruch
Washington, DC
+1.202.739.5219
douglas.baruch@morganlewis.com

- Litigation Partner representing corporations and individuals in a variety of complex civil fraud enforcement matters, including federal and state FCA investigations and litigation.
- Co-author, *Civil False Claims and Qui Tam Actions* (Wolters Kluwer, 5th Ed.), the comprehensive, two-volume treatise that is frequently cited by federal and state courts as an authority on the FCA.