Projecting Privacy and Combating Cyber Fraud: Insights from Recent False Claims Act Settlements under the DOJ's Civil Cyber-Fraud Initiative

Ryan P. Blaney
Partner, Head of Privacy & Cybersecurity
Proskauer Rose LLP

Christopher Terranova
Senior Trial Counsel
Commercial Litigation Branch, Fraud Section
U.S. Department of Justice

Proskauer

Agenda

- Overview of the False Claims Act (FCA)
- Overview of DOJ's Civil Cyber-Fraud Initiative
- Summary of 3 Recent FCA Settlements under DOJ's Initiative
- Trajectory and potential impact of DOJ's Initiative
- Cybersecurity considerations for organizations

Overview of the False Claims Act

Proskauer

"LINCOLN LAW"

The False Claims Act was originally passed in 1863 by President Abraham Lincoln's administration, in response to unscrupulous contractors cheating the government during the Civil War.

False Claims Act: Liability

31 U.S.C. 3729(a)(1) Any person who –

(A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;

(B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;

(C) conspires to commit a violation of subparagraph (A), (B), (D), (E), (F), or (G);

(D) has possession, custody or control of property or money used, or to be used, by the Government and knowingly delivers, or causes to be delivered, less than all of that money or property;

…

(G) Knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay to transmit money or property to the Government.

is liable to the United States Government for a civil penalty of $5,000 – $10,000, as adjusted for inflation, plus 3 times the amount of damages which the Government sustains because of the act of that person.

False Claims Act: Definitions

- **"Knowing" and "knowingly"**
  - A person, with respect to information
    - Has actual knowledge of the information;
    - Acts in deliberate ignorance of the truth or falsity of the information; or
    - Acts in reckless disregard of the ruth or falsity of the information.
  - No proof of specific intent to defraud is required.
- **"Obligation"**
  - An established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment.
- **"Material"**
  - Having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.
- **"Claim"**
  - Any request or demand, whether under contract or otherwise, for money or property and whether or not the United States has title to the money or property that—
    - Is presented to an officer, employee, or agent of the United States; or
    - Is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government—
      - Provides or has provided any portion of the money or property requested or demanded; or
      - Will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded; and
  - Does not include requests or demands for money or property that the Government has paid to an individual as compensation for Federal employment or as an income subsidy with no restrictions on that individual's use of the money or property.

False Claims Act: *Qui Tam* Provisions

- 31 U.S.C. § 3730(b) Actions by Private Persons –
  - (1) A person may bring a civil action for a violation of the FCA for the person and for the United States Government.
- 31 U.S.C. § 3730(d) Award to Qui Tam Plaintiff –
  - (1) Generally 15–25% of proceeds of the action or settlement of claim, if the Government proceeds with the *qui tam* action.
  - (2) Generally 25–30% of proceeds of the action or settlement of claim, if the Government does not proceed with the *qui tam* action.

Overview of DOJ's Civil Cyber-Fraud Initiative

Proskauer

Cybersecurity Executive Order

President Biden issued Executive Order (EO) 14028 on Improving the Nation's Cybersecurity in May 2021.

EO 14028 directed that, among other things, the National Institute of Standards and Technology (NIST):

- Identify existing or develop new standards, tools, and best practices for enhancing software supply chain security; and
- Initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices.

Cybersecurity Executive Order

- Executive Order 14028 also directed that, among other things, the Federal Acquisition Regulatory (FAR) Council publish for public comment proposed updates to the FAR concerning:
  - Standardized contract language for cybersecurity requirements for information technology (IT) and operational technology (OT) service providers; and
  - Contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, software supply chain security requirements.

Civil Cyber-Fraud Initiative (CCFI)

- May 2021: DOJ DAG Lisa Monaco orders comprehensive cyber review.
  - *See* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.
- October 2021: DOJ publicly announces its CCFI.
  - CCFI "will combine [DOJ's] expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems."
    - *See* https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.
- CCFI to use FCA to pursue cybersecurity related fraud by federal contractors and grant recipients.

National Cybersecurity Strategy

- Issued by the White House in March 2023.
- Lists 5 pillars to the national cybersecurity strategy.
- Pillar 3: Shape Market Forces to Drive Security and Resilience.
  - Includes an objective to leverage federal procurement to improve accountability.
  - "When companies make contractual commitments to follow cybersecurity best practices to the Federal Government, they must live up to them."
  - "The [CCFI] uses DOJ authorities under the False Claims Act to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations."

See https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Civil Cyber-Fraud Initiative (CCFI) – cont'd

- CCFI is led by DOJ's Civil Division, Commercial Litigation Branch, Fraud Section.
- Partnering with:
  - Civil Divisions of the 93 U.S. Attorney's offices.
  - Offices of Inspector General and federal agencies across government.
- Builds on existing FCA practice and partnerships.
  - $ Billions each year in recoveries.
  - 600–700 whistleblower suits per year.
- Expected benefits of CCFI:
  1. Building resiliency and improving overall cybersecurity practices.
  2. Holding contractors and grantees to their commitments.
  3. Supporting government experts' efforts to timely identify, create, and publicize patches for vulnerabilities.
  4. Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
  5. Reimbursing the government and taxpayers for losses incurred.

See https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

Civil Cyber-Fraud Initiative (CCFI) – cont'd

- Whistleblowers have a valuable role to play.
  - Under the FCA, private parties can assist the government in identifying and pursing fraudulent conduct and share in any recovery.
- Voluntary disclosures by contractors are encouraged.
  - Under Justice Manual § 4-4.112, credit will be provided to those who voluntarily disclose potential false claims.
  - Credit can also be earned by cooperating with the government investigation and taking remedial action.

Acting AAG Brian Boynton identified at least three common cybersecurity failures that are prime candidates for potential FCA enforcement through CCFI:

1. Knowing failures to comply with cybersecurity standards.
2. Knowing misrepresentation of security controls and practices.
3. Knowing failure to timely report suspected cyber incidents.

See https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and.

1. Knowing Failures to Comply with Cybersecurity Standards

- Acting AAG Brian Boynton: “When government agencies acquire cyber products and services, they often require contractors and grantees to meet specific contract terms, which are often based on uniform contracting language or agency-specific requirements. For example, cybersecurity standards may require contractors to take measures to protect government data, to restrict non-U.S. citizen employees from accessing systems or to avoid using components from certain foreign countries.”
- Currently, many agency-specific cybersecurity requirements exist as a matter of law, policy, or contract.
- EO 14028 directs the FAR Council to propose standardized contract language for appropriate cybersecurity requirements.
- Examples:
  - FAR provisions.
  - Defense FAR Supplement (DFARS) provisions.
  - Homeland Security Acquisition Regulations (HSAR) provisions.
  - NASA FAR Supplement provisions.
  - Research security program standards.

Examples of DFARS Provisions

- Part 239 Acquisition of Information Technology.
  - SUBPART 239.71—SECURITY AND PRIVACY FOR COMPUTER SYSTEMS.
  - SUBPART 239.73—REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK.
  - SUBPART 239.76—CLOUD COMPUTING.
  - 252.239-7000: Protection Against Compromising Emanations.
  - 252.239-7010: Cloud Computing Services.
- SUBPART 204.73: Safeguarding Covered Defense Information and Cyber Incident Reporting.
  - Contractors and subcontractors are required to rapidly report cyber incidents directly to DoD within 72 hours.
  - Required clauses:
    - 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting.
    - 252.204-7009: Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

DFARS 252.204-7012(b) sets minimum requirements for contractors based on whether or not part of an Information Technology (IT) service or system operated on behalf of USG:

- If so, contractor's cloud computing services shall be subject to requirements in clause **252.239-7010** and any other IT services or systems are covered by security requirements in contract
- If not, then, with limited exceptions, "the covered contractor information system shall be subject to the security requirements in **[NIST] Special Publication (SP) 800-171**, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" …in effect at the time the solicitation is issued or as authorized by the Contracting Officer" and the contractor "shall implement NIST SP 800-171, as soon as practical" and provide 30-days notice of "any security requirements specified by NIST SP 800-171 not implemented at the time of contract award" (emphasis added)
- In either case, contractor is ***also*** to apply ***other*** information systems security measures "when ***the Contractor*** reasonably determines" that information systems security measures, in addition to those identified above "may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies ***based on an assessed risk or vulnerability***" (emphasis added)

NIST SP 800-171

Describes 110 security controls (30 “basic” and 80 “derived” requirements).

- “Basic” safeguards track to 14 control families in FIPS-200:

Access Control	Awareness & Training	Audit and Accountability	Configuration Management	Identification and Authentication
Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection
Risk Assessment	Security Assessment	System and Communications Protection	System and Information Integrity	

- “Derived” are from NIST SP 800-53 rev4.
  - *See* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

June 2022 Department of Defense Memorandum

- “The protection of controlled unclassified information on contractor information systems is critically important to the Department of Defense (DoD).”
- “Contractors must implement all of the NIST SP 800-171 requirements and have a plan of action and milestones (per NIST SP 800-171 Section 3.12.2) for each requirement not yet implemented.”
- “Failure to have or to make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of contract requirements.”
  - *See* https://www.acq.osd.mil/dpap/policy/policyvault/USA000807-22-DPC.pdf

2. Knowing Misrepresentation of Security Controls or Practices

- Acting AAG Brian Boynton:
  - "In seeking a government contract, or performing under it, companies often make representations to the government about their products, services, and cybersecurity practices."
  - "These representations may be about a system security plan detailing the security controls it has in place, the company's practices for monitoring its systems for breaches, or password and access requirements."
  - "Misreporting about these practices may cause the government to choose a contractor who should not have received the contract in the first place. Or it could cause the government to structure a contract differently than it otherwise would have."

2. Knowing Misrepresentation of Security Controls or Practices – cont'd

- Examples of misrepresentations or omissions may occur:
  a. In submissions such as system security plans (SSPs) submitted to the Federal Risk and Authorization Management Program (FedRAMP) to receive authorization for cloud-based products.
  b. In disclosures required by contract or regulation, for example:
     – HSAR 3052.204-70(b): "The Contractor shall provide, implement, and maintain an IT Security Plan. . ."
     – NASA FAR Supp. 1852.204-76(c)(4): "Within 30 days after award, the contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer . . ."
  c. In voluntary submissions in connection with offers to sell product or service to a federal agency.
  d. In contractor self-assessments submitted before or during the contract period.

3. Knowing Failure to Timely Report Suspected Cyber Incidents

- Acting AAG Brian Boynton: “Government contracts for cyber products, as well as for other goods and services, often require the timely reporting of cyber incidents that could threaten the security of agency information and systems. Prompt reporting by contractors often is crucial for agencies to respond to a breach, remediate the vulnerability and limit the resulting harm.”

For example, DFARS 252.204-7012:

(a) [. . .] “Rapidly report” means within 72 hours of discovery of any cyber incident.

(c) *Cyber incident reporting requirement*.

(1) 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 shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor’s network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor’s ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.

Three Recent FCA Resolutions

Proskauer

Aerojet Rocketdyne, Inc.

United States ex rel. Markus v. Aerojet Rocketdyne Holdings Inc., No. 2:15-cv-2245 (E.D. Cal.)

- *Qui tam* action filed by former Aerojet employee under the FCA.
- Relator alleged that Aerojet misrepresented its compliance with cybersecurity requirements in certain federal contracts.
- Court denied Aerojet's motion to dismiss – 381 F. Supp. 3d 1240 (E.D. Cal. 2019).
- Court denied in part Aerojet's summary judgment motion – 2022 WL 297093 (E.D. Cal. Feb. 1, 2022).
- Case settled on the second day of trial for $9 million – Relator was awarded $2.61 million share of FCA recovery.
- https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.
- Aerojet provides propulsion and power systems for launch vehicles, missiles, and satellites and other space vehicles to the DoD, NASA, and other federal agencies.
- FCA Allegations Resolved: Misrepresented its compliance with cybersecurity requirements in certain federal government contracts.
  - Alleged failure to disclose and/or remediate multiple data breaches.
  - Allegedly made partial, incomplete disclosures of its compliance, or lack thereof, with security controls.

Comprehensive Health Services LLC

Settlement of two FCA *qui tam* cases:

(1) *United States ex rel. Lawler v. Comprehensive Health Servs., Inc. et al.*, Case No. 20-cv-698 (EDNY) and

(2) *United States ex rel. Watkins v. CHS Middle East, LLC*, Case No. 17-cv-4319 (EDNY).

- CHS is a provider of global medical services that contracted to provide medical support services at government-run facilities in Iraq and Afghanistan.
- Acting AAG Brian Boynton: "This settlement demonstrates the department's commitment to use its civil enforcement tools to pursue government contractors that fail to follow required cybersecurity standards . . ."
- CHS settled FCA allegations for $930,000.
- https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.

Comprehensive Health Services LLC – cont'd

First Set of Allegations Resolved

- CHS submitted claims to the State Department for cost of secure electronic medical record (EMR) system to store confidential patient records for service members, diplomats, officials, and contractors working and receiving medical care in Iraq.
- Between 2012 and 2019, CHS allegedly failed to disclose to the State Department that it had not consistently stored patients' medical records on a secure EMR system.
- When CHS staff scanned medical records for the EMR system, CHS staff saved and left scanned copies of some records on an internal network drive, which was accessible to non-clinical staff.
  - Even after staff raised concerns about the privacy of protected medical information, CHS did not take adequate steps to store the information exclusively on the EMR system.

Comprehensive Health Services LLC – cont'd

First Set of Allegations Resolved

- CHS submitted claims to the State Department for cost of secure electronic medical record (EMR) system to store confidential patient records for service members, diplomats, officials, and contractors working and receiving medical care in Iraq.
- Between 2012 and 2019, CHS allegedly failed to disclose to the State Department that it had not consistently stored patients' medical records on a secure EMR system.
- When CHS staff scanned medical records for the EMR system, CHS staff saved and left scanned copies of some records on an internal network drive, which was accessible to non-clinical staff.
  - Even after staff raised concerns about the privacy of protected medical information, CHS did not take adequate steps to store the information exclusively on the EMR system.

Comprehensive Health Services LLC – cont'd

Second Set of Allegations Resolved

- Under its contracts with the State Department and Air Force, CHS provided medical supplies, including controlled substances, that were approved by the FDA or European Medicines Agency (EMA) and manufactured in accordance with federal quality standards.
- Between 2012 and 2019, CHS allegedly falsely represented to the State Department and Air Force that certain substances provided under its contracts were approved by the FDA or EMA.
  - CHS lacked a DEA license necessary for exporting controlled substances from the U.S. to Iraq.
  - CHS obtained controlled substances by having CHS physicians based in Florida send letters requesting that a South African physician prescribe the controlled substances.
  - A South African shipping company then received controlled substances that were not approved by the FDA or EMA and sent them to CHS in Iraq, where CHS supplied the unapproved controlled substances to patients under the State Department and Air Force contracts.

Jelly Bean Communications Design LLC

Settlement with Jelly Bean and its manager, Jeremy Spinks

- Florida Healthy Kids Corp. (FKHC), which receives federal Medicaid funds, contracted with Jelly Bean to create, host, and maintain the website HealthyKids.org in a HIPAA-compliant environment.
  - Jelly Bean's website included an online application for Medicaid insurance for children.
- Jelly Bean submitted invoices to FKHC for its services, including "HIPAA-compliant hosting."
- However, Jelly Bean allegedly was running multiple outdated and vulnerable applications, including some that it had not updated or patched since 2013, leaving the site and the data vulnerable to attack.
  - In about December 2020, it became apparent that more than 500,000 applications submitted on the website had been hacked, and FKHC shut down the website.
- Jelly Bean and its manager settled FCA allegations for $293,771.
- Principal Deputy AAG Brian Boynton: "We will use the False Claims Act to hold accountable companies and their management when they knowingly fail to comply with their cybersecurity obligations and put sensitive information at risk."
- https://www.justice.gov/opa/pr/jelly-bean-communications-design-and-its-manager-settle-false-claims-act-liability.

Trajectory and Potential Impact of DOJ's Initiative

Proskauer

Expected Benefits of CCFI (Revisited)

- DOJ DAG Lisa Monaco:
  1. Building resiliency and improving overall cybersecurity practices
  2. Holding contractors and grantees to their commitments
  3. Supporting government experts' efforts to timely identify, create, and publicize patches for vulnerabilities
  4. Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage
  5. Reimbursing the government and taxpayers for losses incurred

See https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative

Cybersecurity Considerations for Organizations to Prevent Cyber Fraud and Protect Customer Privacy

Proskauer

Cybersecurity Considerations for Organizations

Understand compliance requirements

- E.g., applicable time period to report cyber incident

Adopt and implement adequate compliance policies and controls.

Train employees on compliance policies and reporting options

Evaluate business partners and third-party vendors

Manage cyber incidents and notification obligations

Have a strong HR system in place, as many whistleblowers first raise concerns internally

Documentation and transparency are important

Additional Resources – CCFI

- Executive Order 14028: Improving the Nation's Cybersecurity (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- DAG Monaco and AAG Kenneth Polite's comments at Cybersecurity Roundtable (Oct. 20, 2021): https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr
- DAG Monaco's speech at ICCS 2022 (July 19, 2022): https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-address-international-conference
- DOJ's Comprehensive Cyber Review, pp. 52-54 (July 2022): https://www.justice.gov/dag/page/file/1520341/download
- DOJ's CCFI webpage: https://www.justice.gov/civil/practice-areas-0#cyberfraud
- DOJ's civil cyber-fraud reporting webpage: https://www.justice.gov/civil/report-fraud
- DOJ's civil fraud section, which includes page discussing FCA: https://www.justice.gov/civil/fraud-section

Thank You

Ryan P. Blaney
Partner, Head of Privacy & Cybersecurity
Proskauer Rose LLP

Christopher Terranova
Senior Trial Counsel
Commercial Litigation Branch, Fraud Section
U.S. Department of Justice

Proskauer