

False Claims Act: Risks for General Counsel Office in 2025

In 2024, the US Department of Justice (DOJ) reported nearly 1,000 qui tam actions, a 37% increase, with the number expected to rise. The False Claims Act (FCA) is a powerful tool that the DOJ utilizes to combat fraud against the federal government. As enforcement priorities evolve and whistleblower activity surges, legal and compliance departments must be proactive and strategic about risk management. This infographic explores key hurdles to organizations, how the FCA guidelines can impact them in 2025, and outlines actionable compliance strategies that the General Counsel (GC) and/or Chief Compliance Officer (CCO) can implement to protect their institutions.

Understanding the compliance risks



1. Expanding the enforcement scope

- Cybersecurity compliance
- Pandemic relief fund
- International trade and procurement (tariffs)

2. Qui tam proliferation and whistleblower risks

- FCA's qui tam provisions allow private individuals to file lawsuits on behalf of the government
- Legal departments must ensure that internal reporting mechanisms are robust, confidential, and trusted by employees

3. Evolving legal standards and judicial trends

- Several federal circuits have adopted a heightened "but-for" causation standard for Anti-Kickback Statute (AKS)-based FCA claims
- The DOJ has defended the constitutionality of the qui tam statute in federal court

4. Reputational and operational fallout

- Suspension or debarment from federal programs
- Shareholder litigation and derivative suits
- Reputational damage that affects customer trust and employee morale

Strategic compliance priorities



- Conduct targeted risk assessments and compliance audits
- Strengthen internal reporting and whistleblower protections
- Proactively evaluate and adjust the compliance program based on enforcement trends and emerging risks
- Prepare for investigations before they happen

Sector-specific considerations



Healthcare

- Medicare Advantage billing practices
- Opioid-related enforcement
- Stark Law and Anti-Kickback Statute compliance

Government contracting

- Cost or pricing data disclosures
- Compliance with Buy American and Trade Agreements Acts
- Cybersecurity certifications and incident reporting

Technology and cybersecurity

- Accurate representations of cybersecurity capabilities
- Timely breach reporting
- Compliance with NIST and CMMC standards



The False Claims Act is not just a legal statute—it is a high-stakes compliance challenge that demands proactive leadership from general counsel. By taking these steps, GCs and CCOs can protect their organizations from the severe consequences of FCA violations and position themselves as strategic advisors in an increasingly complex regulatory environment.

Andrew Bayer, ACCA, CFE, CAMS | Principal, Forensic Services
+1-347-889-3837, abayer@crai.com

CRA's Forensic Services Practice – including our digital forensics, eDiscovery, and cyber incident response lab – is certified under ISO 27001:2022 standards. The Practice has been recognized by *National Law Journal*, *Global Investigations Review*, and ranked by *Chambers*. CRA's clients over the past two years included 98% of the AmLaw 100 law firms, and 85% of the Fortune 100 companies.

CRA Charles River
Associates