THE EXPANDING FALSE CLAIMS ACT: DOJ'S NEW ENFORCEMENT THEORIES AND WHAT FEDERAL CONTRACTORS MUST KNOW

Date: 17 June 2026

US Policy and Regulatory Alert

By: Nora E. Becerra

EXECUTIVE SUMMARY

For decades, the False Claims Act (FCA) has served as the government's primary tool for combating fraud involving federal funds. FCA enforcement has historically focused on well-established fraud theories such as overbilling, defective pricing, medically unnecessary services, and the submission of false invoices. However, over the last decade, the government and relators have increasingly advanced more novel and expansive theories of FCA liability, reflecting an evolution in enforcement priorities and a willingness to test the statute's boundaries.

That evolution has been accompanied by significant enhancements in enforcement capabilities. Today, the Department of Justice (DOJ) is increasingly leveraging artificial intelligence (AI), data analytics, interagency information-sharing, and specialized enforcement task forces to identify potential FCA violations. At the same time, DOJ has expanded its focus to a broader range of compliance-related conduct. This heightened enforcement landscape has coincided with record-breaking FCA recoveries. In January 2026, DOJ reported US$6.8 billion in FCA recoveries for Fiscal Year (FY) 2025, marking the largest annual total to date.[1]

While healthcare-related matters continue to account for a substantial share of recoveries, procurement fraud remains a major enforcement priority. In FY 2025, DOJ secured its second-largest procurement fraud recovery in history, when a federal contractor agreed to pay US$428 million to resolve allegations involving false cost and pricing data and double-billing on a weapons maintenance contract with the US Department of Defense (DOD).[2]

More recently, procurement enforcement has extended beyond pricing and billing disputes to alleged failures to comply with contractual and regulatory certifications. DOJ has increasingly pursued FCA theories based on cybersecurity requirements, diversity, equity, and inclusion certifications, domestic sourcing and supply chain obligations, and other regulatory certifications made in connection with government contracts.

This expansion shows no signs of subsiding. DOJ's establishment of the National Fraud Enforcement Division on 7 April 2026 underscores a continued institutional focus on fraud detection and coordination.[3] Increasingly, DOJ is examining not only what contractors bill, but also what they certify. As a result, representations made in proposals, certifications, compliance reports, questionnaires, and contract performance submissions may carry significant FCA exposure if later alleged to be inaccurate or unsupported—even in the absence of traditional billing misconduct or an underlying loss event.

©2005-2026 K&L Gates LLP. All Rights Reserved.

For federal contractors, these developments reflect a broader risk environment in which compliance obligations once viewed as straightforward operational or administrative requirements have evolved into an enterprise-wide risk that implicates legal, compliance, cybersecurity, human resources, operations, and executive leadership.

THE EVOLUTION OF FCA ENFORCEMENT

The government's modern FCA enforcement strategy is increasingly centered on certifications, representations, and compliance commitments made in connection with federal funding and contract performance. For example, rather than focusing solely on whether a contractor submitted an inaccurate invoice, DOJ is examining whether contractors knowingly represented compliance with requirements that the government considers material to payment or continued participation in a federal program.

This trend is rooted in the FCA's "implied certification" theory, which the Supreme Court recognized in *Universal Health Services v. United States ex rel. Escobar*.[4] Under that framework, a contractor may face FCA liability where it knowingly misrepresents compliance with requirements that are material to the government's payment decision or continued participation in a federal program.

As a practical matter, this means contractors may face scrutiny not only for submitting false claims for payment, but also for certifying compliance with contractual, regulatory, or statutory requirements that the government considers significant.

Several recent DOJ initiatives demonstrate how this enforcement theory is being applied in practice.

Cybersecurity Compliance as an FCA Issue

One of the most significant developments has been DOJ's continued use of its Civil Cyber-Fraud Initiative[5] to pursue contractors that allegedly misrepresented their cybersecurity practices.

Under this initiative, originally announced in October 2021, DOJ has focused on situations where contractors allegedly:

- Certified compliance with cybersecurity requirements that had not been fully implemented;
- Failed to disclose known cybersecurity deficiencies;
- Submitted inaccurate responses during security assessments or audits;
- Misrepresented the effectiveness of cybersecurity controls; or
- Failed to satisfy contractual obligations relating to safeguarding government information.

Notably, these cases do not necessarily require a data breach or cybersecurity incident. Instead, the government's theory often centers on whether a contractor knowingly made false or misleading statements regarding its cybersecurity posture. In FY 2025 alone, DOJ recovered over US$52 million in nine settlements under the Civil Cyber-Fraud Initiative, with cybersecurity-related settlements more than tripling in each of the past two years.[6]

As cybersecurity obligations continue to expand through frameworks such as National Institute of Standards and Technology (NIST) standards, Cybersecurity Maturity Model Certification requirements, agency-specific security

©2005-2026 K&L Gates LLP. All Rights Reserved.

clauses, and contractual certifications, contractors should expect increased scrutiny of cybersecurity representations made throughout both the procurement and performance lifecycle.

Civil Rights Compliance and the FCA

DOJ has also expanded its use of the FCA through its Civil Rights Fraud Initiative, which focuses on situations where recipients of federal funds allegedly make false certifications regarding compliance with applicable civil rights laws and regulations.

Although enforcement in this area remains relatively new, the initiative signals DOJ's willingness to test the FCA as a vehicle for enforcing civil rights compliance certifications that historically may have been addressed through administrative or regulatory mechanisms. To that end, DOJ entered into its first FCA resolution under the Civil Rights Fraud Initiative with a government contractor in April 2026, wherein the contractor agreed to pay US$17 million to resolve allegations of failure to comply with anti-discrimination requirements in its federal contracts.[7]

For contractors, the significance extends beyond any particular substantive requirement, and the broader lesson is that certifications concerning compliance programs, policies, and operational practices are increasingly becoming focal points of FCA scrutiny.

Procurement Integrity and Performance-Based FCA Theories

Traditional procurement fraud remains a major enforcement priority, but DOJ has increasingly expanded its focus beyond post-award billing disputes to encompass representations made throughout the procurement lifecycle, including during solicitation, award, and performance.

Recent enforcement activity has addressed a widening range of alleged misrepresentations and compliance failures, including:

- Defective pricing and cost or commercial item disclosures;
- Small business and socioeconomic program eligibility certifications;
- Buy American and domestic sourcing requirements;
- Labor and wage compliance certifications;
- Quality control, testing, and product specification representations; and
- Contract performance metrics reported to government customers.

Taken together, these developments are illustrated in recent DOJ resolutions involving alleged misstatements in cost and pricing data, as well as cybersecurity and program-compliance matters, in which the government has advanced the theory that ongoing compliance obligations are material to the government's decision to pay for, or continue performance under, a contract. While courts continue to apply the materiality standard articulated in Escobar, these cases reflect DOJ's increasingly aggressive use of certification-based theories in the procurement context.

As noted above, recent cybersecurity-related FCA settlements brought under the Civil Cyber-Fraud Initiative have alleged that misrepresentations regarding required security controls go directly to the government's decision to pay for or continue performance under a contract. These cases illustrate DOJ's view that compliance

©2005-2026 K&L Gates LLP. All Rights Reserved.

representations made during performance may be evaluated as material to payment decisions, particularly where they are expressly incorporated into contract terms or certification regimes.

MATERIALITY REMAINS THE KEY LIMITING PRINCIPLE

Despite the expansion of FCA theories, not every regulatory or contractual violation creates FCA liability.

The Supreme Court's decision in Escobar emphasized that materiality is a demanding standard. To establish liability, the government generally must show that the alleged noncompliance was material to the government's decision to pay claims or continue participation in a federal program. In the wake of *Escobar*, numerous federal circuit courts now apply a holistic analysis to determine whether an alleged noncompliance was truly material, considering factors such as whether compliance is expressly designated as a condition of payment, whether the requirement goes to the essence of the bargain, and whether the government continues to pay claims despite knowledge of noncompliance. No single factor is dispositive, and materiality is ultimately a context-specific inquiry.[8]

Nevertheless, recent enforcement activity suggests that the government increasingly advances theories of materiality grounded in the centrality of compliance obligations to payment decisions, particularly in areas such as cybersecurity, data protection, procurement certifications, and program integrity controls. For example, a university paid US$1.25 million to resolve FCA allegations arising from alleged failures to comply with cybersecurity requirements under DOD contracts in October 2024,[9] and since then at least eight additional settlements have involved alleged failures to implement NIST-based controls, maintain system security plans, or address identified cybersecurity vulnerabilities, even in the absence of a breach or confirmed access by a threat actor.

Contractors therefore should focus not only on whether they are compliant, but also on whether compliance representations accurately reflect operational realities.

WHISTLEBLOWER ACTIVITY CONTINUES TO DRIVE ENFORCEMENT

Many of the DOJ's most significant FCA matters originate from whistleblower complaints filed by current or former employees, subcontractors, consultants, or competitors. In FY 2025, whistleblowers filed nearly 1,300 FCA lawsuits, the highest number in a single year.[10] These complaints will likely remain the primary source of FCA investigations.

At the same time, FCA enforcement is becoming increasingly data-driven. Whistleblowers and the government are increasingly using data analytics and AI-enabled tools to identify alleged billing anomalies, pricing discrepancies, utilization patterns, contract performance issues, and other indicators of potential noncompliance.

As a result, organizations should expect whistleblower allegations to be supported by increasingly detailed analyses of internal and publicly available data, making it easier for whistleblowers to identify potential FCA theories. For more detail, please see our recent alert regarding DOJ's new Fraud Oversight through Careful Use of Statistics Initiative for data miners filing FCA lawsuits.

As FCA enforcement theories continue to expand beyond traditional billing disputes, organizations should expect whistleblowers to focus on:

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Internal audit findings;
- Compliance assessments;
- Cybersecurity reviews;
- Quality assurance reports;
- Regulatory deficiencies;
- Contract performance metrics;
- Internal investigations; and
- Management communications concerning known compliance issues.

Organizations should assume that internal compliance documentation, operational data, and performance metrics may become central evidence in future FCA investigations or litigation. Companies should also recognize that data that may appear routine when viewed in isolation can be leveraged by whistleblowers and enforcement authorities to identify patterns that support broader allegations of fraud or noncompliance.

PRACTICAL CONSIDERATIONS FOR FEDERAL CONTRACTORS AND NEXT STEPS

The expanding scope of FCA enforcement creates several practical risks for contractors that should be addressed proactively.

First, legal and compliance teams should recognize that representations made in proposals, certifications, questionnaires, compliance reports, and contract deliverables may receive the same scrutiny historically reserved for invoices and payment requests.

Second, organizations should ensure that compliance functions are adequately integrated into contract performance and governance processes.

Third, contractors should assess whether internal controls can identify situations in which contractual commitments differ from actual practices.

Finally, leadership should recognize that FCA risk increasingly extends beyond finance and billing functions and now encompasses cybersecurity, privacy, human resources, regulatory compliance, quality assurance, and operational performance.

Accordingly, contractors should consider the following next steps:

- Inventory significant certifications and compliance representations made to government customers;
- Validate that contractual obligations are mapped onto operational controls and business processes;
- Establish governance procedures for reviewing compliance certifications before submission;
- Ensure that identified compliance gaps are documented, escalated, and remediated appropriately;

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Evaluate whether cybersecurity, quality assurance, human resources, and operational compliance functions are integrated into enterprise risk management processes; and
- Review whistleblower reporting and investigation procedures to ensure concerns are addressed promptly and consistently.

CONCLUSION

Recent DOJ initiatives demonstrate that FCA enforcement increasingly extends beyond traditional billing and pricing fraud to encompass certification and other compliance-related obligations. As DOJ continues to expand its use of data analytics, AI, and specialized enforcement initiatives, contractors should expect heightened scrutiny of representations relating to cybersecurity, civil rights compliance, supply chain requirements, quality assurance, and contract performance.

In this evolving enforcement environment, organizations should carefully evaluate whether their compliance programs, internal controls, and government-facing representations accurately reflect operational realities.

FOOTNOTES

[1] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., *False Claims Act Settlements and Judgements Exceed $6.8B in Fiscal Year 2025* (Jan. 16, 2026), https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-68b-fiscal-year-2025.

[2] Press Release, U.S. Att'y's Off., Dist. of Mass., *Raytheon Agrees to Pay Over $950 Million in Connection with Defective Pricing, Foreign Bribery and Export Control Schemes* (Oct. 16, 2024), https://www.justice.gov/usao-ma/pr/raytheon-agrees-pay-over-950-million-connection-defective-pricin…; *see also* Settlement Agreement, *United States ex rel. Atesoglu v. Raytheon Techs. Corp., No. 21-CV-10690-PBS* (D. Mass. Oct. 16, 2024), https://www.justice.gov/d9/2024-10/settlement_agreement_1.pdf.

[3] Press Release No. 26-328, U.S. Dep't of Just., Off. of Pub. Affs., *Acting Attorney General Todd Blanche Issues Memorandum on the Creation of the National Fraud Enforcement Division* (Apr. 7, 2026), https://www.justice.gov/opa/pr/acting-attorney-general-todd-blanche-issues-memorandum-creation-national-fraud-enforcement.

[4] *Universal Health Servs., Inc. v. United States ex rel. Escobar*, 579 U.S. 176 (2016).

[5] Press Release No. 21-971, U.S. Dep't of Just., Off. of Pub. Affs., *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative* (Oct. 6, 2021), https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[6] U.S. Dep't of Just. *Fact Sheet: False Claims Act Settlements and Judgements—FY 2025* (Jan. 16, 2026), https://www.justice.gov/opa/media/1424126/dl.

[7] U.S. Dep't of Just., Off. of Pub. Affs., *IBM Pays $17 Million to Resolve Allegations of Discrimination Through Illegal DEI Practices* (Apr. 10, 2026), https://www.justice.gov/opa/pr/ibm-pays-17-million-resolve-allegations-discrimination-through-illegal-dei-practices.

©2005-2026 K&L Gates LLP. All Rights Reserved.

[8] *See, e.g., United States ex rel. Zotos v. Town of Hingham,* 98 F.4th 339 (1st Cir. 2024); *United States ex rel. Druding v. Care Alts.*, 81 F.4th 361 (3d Cir. 2023); *United States ex rel. Prather v. Brookdale Senior Living Cmtys.*, 892 F.3d 822 (6th Cir. 2018); *United States ex rel. Holt v. Medicare Medicaid Advisors, Inc.*, 115 F.4th 908 (8th Cir. 2024); *United States ex rel. Campie v. Gilead Scis., Inc.*, 862 F.3d 890 (9th Cir. 2017); *United States ex rel. Janssen v. Lawrence Mem'l Hosp.*, 949 F.3d 533 (10th Cir. 2020).

[9] U.S. Dep't of Just., Off. of Pub. Affs., *The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements* (Oct. 22, 2024), https://www.justice.gov/archives/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating.

[10] *See supra* note 1.

KEY CONTACTS



NORA E. BECERRA
PARTNER

CHICAGO
+1.312.807.4222
NORA.BECERRA@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.