BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

A New Era Of Corporate Fraud Liability: The UK's Failure To Prevent Fraud Offense Meets The U.S. False Claims Act

By Matthew Banham, Edward V. "Teddie" Arnold, and Sarah E. Barney[*]

Executive Summary

The United Kingdom's Failure to Prevent Fraud (FTPF) offense,[1] effective September 1, 2025,[2] represents a significant expansion of corporate criminal liability. The offense applies to "large" organizations and imposes liability where an employee, agent, subsidiary, or other associated person commits fraud intending whether directly or indirectly to benefit the organization. Senior management knowledge is not required and the offense has extraterritorial reach wherever the conduct or its effects have a UK nexus. The sole defense is for the organization to demonstrate that it maintained "reasonable procedures" to prevent fraud, assessed against six principles set out in statutory guidance.[3]

By contrast, the U.S. False Claims Act (FCA)[4] imposes civil liability for knowingly submitting false or fraudulent claims to the federal government. Through its *qui tam* regime, the FCA empowers whistleblowers to initiate enforcement actions and share in financial recoveries,[5] making it one of the most potent compliance and enforcement tools in the United States. Recent Department of Justice initiatives including the Civil Cyber-Fraud Initiative[6] and expanded cooperation credit policies[7] further extend the statute's reach and strengthen expectations for voluntary disclosure and proactive remediation.

For U.S.-headquartered multinational corporations the emergence of the

[*]*Matthew Banham is a Partner in Seyfarth Shaw's London office whose practice focuses on white-collar defense, cross-border investigations, global compliance, and workplace investigations. Teddie Arnold is a Partner in Seyfarth's Government Contracts practice group in Washington, D.C. and assists contractors with all aspects of government procurement, including bid protests, contract claims, internal investigations, ethics and compliance, data rights and intellectual property, procurement fraud, small business issues, and transactional matters. He also co-leads the firm's False Claims, Whistleblower, and Internal Investigations group. Sarah Barney is an Associate in Seyfarth Shaw's Government Contracts practice group. Her practice focuses on bid protests, regulatory compliance counseling, and internal investigations.*

IN THIS ISSUE:

FTPF offense introduces overlapping compliance obligations: the need to manage significant civil and criminal exposure under the FCA alongside criminal exposure in the UK associated with the FTPF offense. This BRIEFING PAPER examines the civil FCA only, but both frameworks reflect a common regulatory trend toward preventive controls, strong internal governance, and active oversight of employees, subsidiaries, and third-party intermediaries.

Introduction

The establishment of the FTPF offense and the continuing evolution of FCA enforcement reflects a global trend toward enhanced corporate accountability for economic crime. While the FTPF constitutes a strict-liability corporate criminal offense, the FCA operates as a civil statute grounded in knowledge-based liability and whistleblower participation. Despite these doctrinal differences, both regimes lower evidentiary barriers traditionally associated with prosecuting or pursuing claims against complex corporate entities.

For multinational corporations, particularly those operating in regulated sectors or engaged in government procurement, these developments impose significant compliance and governance demands. The FTPF's extraterritorial provisions expose non-UK organizations to criminal liability where fraud occurs in or impacts the UK. Likewise, the FCA's expansive definition of "claims" and its incentive structures afforded to whistleblowers create substantial civil exposure. Consequently, organizations must develop and implement coordinated cross-jurisdictional compliance frameworks capable of addressing evolving fraud risks while meeting increasing expectations of transparency and internal reporting.

This BRIEFING PAPER provides a comparative analysis of the FTPF and FCA civil regime with a particular focus on the implications for government contractors and multinational enterprises.

Legislative Background

United Kingdom: Failure To Prevent Fraud (FTPF)

The FTPF offense, introduced by the Economic Crime and Corporate Transparency Act 2023,[8] substantially enhances the corporate criminal liability landscape in the UK. Under the regime, "large" organizations are criminally liable when an "associated person," defined to include employees, agents, subsidiaries, and other service providers, commits fraud intending to benefit the organization or, in certain circumstances, its clients. The definition of "associated person" is contextual rather than contractual.[9] The perpetrator's motive need not be solely or primarily to benefit the organization; indirect benefit may suffice.[10] Crucially, liability does not require senior management involvement, reflecting Parliament's effort to overcome challenges associated with attributing fault within complex structures.

The sole statutory defense to the FTPF offense requires organizations to demonstrate that they maintained "reasonable procedures" to prevent fraud.[11] The procedures are anchored in six defined principles: top-level commitment, risk assessment, proportionate procedures, due diligence, communication and training, and monitoring and review.[12]

The offense also has significant extraterritorial reach. Organizations incorporated outside the UK may face li-

Editor: Valerie L. Gross

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

ability where the underlying fraud occurs within the UK or has a UK nexus.[13] Enforcement bodies, including the Serious Fraud Office (SFO), have already signaled an intention to pursue early cases which, through the courts, will help to establish precedent and operational clarity.

United States: False Claims Act

The FCA is the U.S. government's principal civil mechanism for combating fraud involving public funds. Liability arises where an individual or entity knowingly submit false or fraudulent claims for payment or approval to a federal entity or recipients of federal funds with liability established through evidence of falsity, knowledge, materiality, and presentment.[14] Although civil in nature, the FCA carries severe financial consequences, including treble damages and statutory penalties imposed on government contractors, subcontractors, or suppliers. The FCA defines a variety of fraudulent schemes that come under the Act's purview, but the essential elements of an FCA claim are that (1) there is a claim; (2) the claim was false (either by misrepresentations or omissions); (3) the claim was submitted knowingly for payment or reimbursement; and (4) the claim was material.

The FCA's modern enforcement architecture is shaped largely by the 1986 amendments, which strengthened whistleblower (*qui tam*) provisions and broadened the scope of actionable conduct.[15] Under the *qui tam* mechanism, whistleblowers (also known as relators) may bring actions on behalf of the U.S., although the U.S. Department of Justice (DOJ) may intervene in these actions, and they may receive between 15% and 30% of any financial recovery.[16] These incentives have contributed towards a substantial volume of enforcement activity: in fiscal year 2024, whistleblowers filed 979 *qui tam* actions, contributing to the majority of the $2.9 billion in government recoveries.[17] DOJ policies on voluntary self-disclosure of FCA violations emphasize proactive and timely reporting and in return offer reduced penalties.[18] These developments increasingly align the FCA's underlying philosophy with the preventive, governance-oriented approach embedded in the FTPF regime.

The FCA's enforcement focus continues to expand. The Civil Cyber-Fraud Initiative applies FCA liability theories to companies providing certain forms of deficient cybersecurity products or services to the government and failing to comply with regulatory or contractual requirements by knowingly misrepresenting cybersecurity practices and protocol or failing to report cybersecurity incidents.[19]

Scope And Applicability

United Kingdom

The FTPF offense applies only to "large organizations."[20] An organization qualifies as "large" if it meets at least two of the following criteria:

- more than 250 employees,
- more than £36 million in turnover, or
- more than £18 million in total assets.[21]

These thresholds apply across corporate groups irrespective of geographic footprint. Subsidiaries that independently meet the threshold qualify as "relevant organizations" and may be prosecuted. Subsidiaries that do not meet the threshold may still be liable if their employees commit fraud intending to benefit the subsidiary. Small and Medium Enterprises (SMEs), although outside direct liability, often function as "associated persons" to larger entities and must therefore elevate their fraud controls to maintain commercial relationships. For U.S. contractors, this effectively extends third-party program expectations deep into UK-facing supply chains.[22]

United States

By contrast, the FCA contains no size threshold. It applies to any individual or entity that submits, or causes the submission of, claims for payment to the federal government or to recipients of federal funds.[23] This includes contractors, subcontractors, suppliers, grantees, and other downstream entities. The FCA's broad scope reflects its purpose as a universal safeguard against fraud involving federal expenditures.

Types Of Fraud Covered

United Kingdom

The FTPF offense targets specific fraud-related crimes, including false representations, failure to disclose information, and making misleading statements to the market.

It also encompasses cheating the public revenue, false statements by a company director, and false accounting.[24] Liability arises only where the fraud is committed by an "associated person" acting in that capacity and intending to benefit the organization or its clients.[25]

United States

The FCA applies to any false or fraudulent claims for payment or approval under federal programs.[26] This expansive approach is reflected in the Act's broad definition of a "claim," which includes any requests or demands for money or property that is:

- presented to an officer, employee, or agent of the U.S.;
- made to a contractor, grantee, or other recipient of federal funds; or
- submitted to any entity where the requested funds will be reimbursed with federal money.[27]

As a result, the FCA captures a wide range of conduct, including:

- false certifications of compliance with federal requirements (such as cybersecurity obligations[28] or domestic sourcing rules[29]);
- inflated billing or billing for unnecessary or unperformed services;[30]
- inaccurate certifications to obtain COVID-19 relief funds, including overstated payroll, revenue, or business losses.[31]

In addition to affirmative misrepresentations, the FCA also encompasses material omissions where the failure to disclose information renders a claim misleading.[32]

Unlike the FTPF, FCA liability does not require organizational benefit. The focus is on whether the defendant knowingly submitted a false claim and whether the falsehood was material to the government's payment decision; whether the entity ultimately profited is irrelevant.[33]

The FCA's broad reach, grounded in the involvement of federal funds, allows it to encompass diverse schemes resulting in financial loss to the government. This expansive scope has practical implications for borderline cases involving administrative error, ambiguous contractual terms, or evolving regulatory obligations. It also explains why certification regimes (cybersecurity, domestic preference, pricing, eligibility) and subcontractor oversight remain central pillars of U.S. government contract compliance frameworks.

Jurisdiction

United Kingdom

The FTPF offense exposes organizations incorporated or formed outside the UK to prosecution if the fraud has a UK nexus and was committed by an associated person of the organization. A UK nexus may arise when losses occur in the UK, UK nationals are impacted, or an element of the offense took place in the UK.[34] This broad jurisdictional scope means that multinational organizations must ensure that their global compliance programs meet UK standards.

United States

The FCA applies globally wherever U.S. federal funds are implicated. Multinational corporations frequently face FCA exposure through direct contracting, subcontracts, grant funding, or participation in supply chains where federal reimbursement is expected.

Legal Defenses

UK: Reasonable Procedures

A central feature of the FTPF offense is the availability of a full defense if the organization can prove it had "reasonable procedures" in place to prevent fraud.[35] The government's guidance outlines six principles for such procedures.[36] These principles mirror those found in the Bribery Act 2010 guidance and emphasize a proactive, risk-based approach to compliance.[37]

1. Top-Level Commitment: Senior management must foster a culture of integrity and compliance.
2. Risk Assessment: Organizations should periodically assess fraud risks relevant to their operations.
3. Proportionate Procedures: Anti-fraud measures should be tailored to the organization's size, structure, and risk profile.

4. Due Diligence: Vetting of third parties and associated persons is essential.

5. Communication and Training: Staff and associated persons must be informed and trained on fraud risks and procedures.

6. Monitoring and Review: Procedures should be regularly reviewed and improved based on experience and evolving risks.

The guidance stresses that there is no one-size-fits-all solution. It requires a dynamic and evidence-based approach. Organizations must be able to demonstrate not only that procedures exist, but that they are embedded in the organization's day-to-day operations, regularly tested, and adapted to emerging risks. Organizations should refresh their fraud policies and risk assessment documents regularly, especially as changes to an organization's supply chains or practices evolve. This guidance further encourages organizations to record the reasons for an entity's decisions, risk matrices, and compliance efforts to evidence their reasonable procedures. In practical terms, UK prosecutors will expect the organization to have management information including board minutes, Key Performance Indicators, testing logs, training records, and exception analyses that demonstrate the program works in practice.[38]

U.S.: Qui Tam Provisions And Penalties

One of the FCA's most distinctive features is its *qui tam* mechanism that allows private individuals (relators) to file lawsuits on behalf of the government. If successful, relators may receive between 15% and 30% of the recovered funds, depending on whether the government intervenes.[39] This incentive structure has led to a surge in whistleblower activity (with an all-time high of 979 *qui tam* cases filed in fiscal year 2024) and has been instrumental in uncovering large-scale fraud.[40] The *qui tam* mechanism capitalizes on the fact that individuals, such as an organizations employees, may be in the best position to raise the alarm bells about fraud.

Penalties under the FCA are severe. Defendants found liable may be required to pay treble damages (three times the amount of the government's loss), which can quickly escalate recovery into the millions of dollars.[41] Additionally, violation of the FCA may serve as the basis for suspension or debarment of an organization from government contracting.[42] DOJ has publicly prioritized FCA enforcement in sectors such as healthcare, defense, and cybersecurity, often leveraging data analytics and interagency cooperation.

Recent DOJ policy updates have emphasized the importance of corporate cooperation and self-disclosure in mitigating the damage of a known FCA violation. DOJ has released guidelines for self-disclosure of FCA violations and indicated that entities that make "proactive, timely, and voluntary" disclosures will receive credit during the resolution of an FCA case.[43]

Additionally, DOJ's Civil Cyber-Fraud Initiative has signaled a new wave of FCA enforcement targeting cybersecurity noncompliance in government contracts.[44] For the first time since the launch of the Civil-Cyber Fraud Initiative, in fiscal year 2024 the DOJ intervened in a cybersecurity case alleging that a public research university failed to develop and implement a security plan as required by Department of Defense cybersecurity regulations and submitted an inaccurate cybersecurity claim.[45] Legal advisors must now consider FCA exposure in areas previously seen as technical or operational rather than legal.

Beyond *qui tam*, DOJ's Corporate Whistleblower Awards Pilot Program (Criminal Division) provides monetary awards tied to forfeiture for information on specified corporate crimes, increasing incentives to report and reinforcing the value of robust internal reporting channels.[46] The UK is also moving toward U.S.-style tax whistleblower rewards for HM Revenue & Customs (HMRC) investigations and there is a call for financial incentives across all corporate criminal offenses signaling a cultural shift toward incentives in economic crime enforcement.[47]

Practical Implications For Government Procurement

Both the UK FTPF and the U.S. FCA regimes impose heightened expectations on government contractors and affirm the importance of a culture of compliance. Organizations must go beyond formal policies and foster an environment where ethical conduct is expected, supported, and enforced. Failure to do so can result in

reputational damage, financial penalties, and debarment from future government contracts.

In the UK, procuring bodies may require evidence of anti-fraud frameworks. This could include internal policies, training records, risk assessments, and audit trails. Weak procedures may result in reputational harm, disqualification from tenders or criminal prosecution.

In the U.S., the FCA has long required rigorous internal controls, accurate certifications, and strong oversight of subcontractors. The risk of whistleblower actions means that internal controls, employee training, and reporting mechanisms are essential. Contractors must also be vigilant in subcontractor oversight, as liability can extend to false claims submitted by downstream partners.

Across both jurisdictions, enforcement actions are often publicized, and organizations may face suspension or debarment from future contracts. As such, proactive compliance is not only a legal safeguard but also a competitive advantage in public procurement markets.

Comparative Trends And Legal Convergence

Key Trends

The UK's new offense and the U.S. FCA reflect a broader global trend towards corporate accountability and proactive fraud prevention. Several key trends emerge from a comparative analysis:

- *Expansion of Corporate Liability*: Both regimes attribute liability to organizations for actions of associated persons. This reflects a shift from individual culpability to institutional responsibility.
- *Emphasis on Preventive Measures*: The FTPF's reasonable procedures defense and the FCA's focus on internal controls underscore a preventive philosophy. Regulators expect organizations to anticipate and mitigate fraud risks.
- *Whistleblower Empowerment*: While the UK lacks a formal *qui tam* mechanism the operating landscape in the UK is changing. HMRC (the UK body responsible for tax evasion and civil enforcement of trade sanctions) has announced the introduction of formal incentive program modeled on the highly successful U.S. Internal Revenue Service (IRS) Whistleblower Program.[48] This is alongside calls by the SFO for a whistleblowing model similar to the DOJ Corporate Whistleblower Awards Pilot Program.[49]
- *Cross-Border Enforcement*: Multinational organizations operating in both jurisdictions must navigate overlapping compliance obligations. Coordination between UK and U.S. enforcement agencies is commonplace particularly in sectors like defense, healthcare, and financial services.
- *Sector-Specific Focus*: Both regimes prioritize enforcement in high-risk sectors. In the U.S., this includes healthcare fraud, defense contracting, COVID-19 relief programs, and cybersecurity. In the UK, early enforcement is expected in financial services, construction, and public infrastructure.
- *Compliance Alignment*: To mitigate risk under both regimes, organizations should demonstrate their awareness of business-relevant risks and have in place mitigation measures that are actively monitored, tested, and effective across the three lines of defense. Culture is the foundation of compliance, and it must be embedded across the organization, with sustainable behaviors and shared responsibility.

These trends suggest that organizations must adopt a holistic, risk-based approach to advising clients. Compliance is integral to strategic decision-making and corporate governance.

Issue	UK (FTPF)	US (FCA)
Enforcement Mechanism	Criminal	Civil[50]
Whistleblower Involvement	No financial incentives	Strongly incentivized via financial compensation (*qui tam*)
Jurisdiction	Applies globally if fraud has UK nexus	Applies globally to claims that implicate the payment or reimbursement of federal funds
Defense	Reasonable procedures	No intent, no knowledge, immateriality
Sector Focus	All sectors	Healthcare, defense, cyber, education

Notable Divergences

Both laws reflect a convergence toward preventive compliance, corporate responsibility, and sector-focused enforcement. However, notable divergences remain:

- The U.S. uses civil monetary penalties and whistleblower incentives; the UK emphasizes criminal deterrence and procedural rigor.
- The FCA's materiality standard is evolving through litigation; the FTPF is likely to develop through early SFO prosecutions.
- Multinational firms must harmonize fraud prevention frameworks across both jurisdictions to minimize duplication and avoid legal gaps.

Risk Prevention Guidelines

The FTPF offense requires large organizations to reassess their internal controls especially in high-risk sectors like financial services, construction, and public procurement. Rather than relying on generic policies, organizations must tailor their procedures to reflect their specific risk profiles. Crucially, the offense extends beyond internal conduct. Organizations must now consider outward-facing activities, including the actions of third parties acting on their behalf. This calls for a broader and more rigorous approach to risk assessment. While existing controls and frameworks such as anti-bribery and corruption (ABC) risk assessments can be adapted, they should not be relied on blindly. New and evolving risks must be taken into account. Though workshops with business units may take more time, they are often the most effective way to uncover potential weaknesses.

Risk management must go beyond financial controls and remain dynamic to business changes. Functions like marketing, sales, hospitality, and sustainability should also be integrated into the compliance framework. Organizations must document their methodologies, decisions, and controls, ensuring their compliance plans are dynamic and responsive. These plans should reflect a clear understanding of the organization's route to market and its various distribution channels. Similarly, as changes are made to those channels or the supply chain, the risk management procedures should be revisited to ensure they account for new or changed liability. Senior management must be fully aware of the controls in place and the risks they are designed to mitigate.

Finally, organizations must prepare for the FTPF offense. A clear and well-established plan should be in place for escalation, investigation, and remediation when things go wrong. As a result, outside counsel and in house compliance employees should consider the following steps. Bear in mind, however, that these recommendations are not a substitute for professional representation in any specific situation.

1. *Conduct a Fraud Risk Assessment*: Identify and assess fraud risks specific to their operations, particularly in relation to government contracts.

2. *Implement Reasonable Procedures*: Develop and document anti-fraud procedures aligned with the UK guidance's six principles.

3. *Review and Update Compliance Programs*: Verify that FCA and FTPF compliance programs are current, effective, and tailored to the organization's risk profile.

4. *Train Staff and Associated Persons*: Provide regular training on fraud risks, reporting mechanisms, and legal obligations under both UK and U.S. law.

5. *Establish Whistleblower Protocols:* Implement clear procedures for handling internal whistleblower reports and protecting whistleblowers from retaliation.

6. *Monitor Third-Party Relationships*: Conduct due diligence on subcontractors and partners, and include fraud prevention clauses in contracts.

7. *Document Decisions*: Maintain audit trails, document compliance efforts, and be ready to respond to investigations or enforcement actions.

8. *Engage With Procurement Authorities*: Demonstrate compliance during bidding processes and responding to due diligence inquiries.

9. *Coordinate Across Jurisdictions*: For multinational organizations harmonize compliance efforts to meet both UK and U.S. standards, avoiding duplication and gaps.

10. *Stay Informed*: Monitor legal developments, enforcement trends, and guidance updates to ensure clients remain compliant and competitive.

Conclusion

The FTPF offense mirrors the FCA's emphasis on organizational responsibility but is more severe given its criminal nature and expansive attribution model through the "associated persons" definition and its broad jurisdictional reach. The FCA continues to drive significant civil recoveries supported by whistleblower incentives and emerging DOJ initiatives.

For multinational corporations, harmonizing fraud-prevention frameworks across jurisdictions is no longer optional—it is essential to strategic risk management and sustainable participation in government procurement markets.

ENDNOTES:

[1]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199 (U.K.).

[2]UK Home Office, Economic Crime and Corporate Transparency Act 2023: Guidance to organizations on the offense of failure to prevent fraud (accessible) § 1.3 (updated Oct. 10, 2025), https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version.

[3]UK Home Office, Economic Crime and Corporate Transparency Act 2023: Guidance to organizations on the offense of failure to prevent fraud (accessible) (updated Oct. 10, 2025) https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version.

[4]31 U.S.C.A. §§ 3729–3733.

[5]31 U.S.C.A. § 3730.

[6]Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa A. 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.

[7]U.S. Dep't of Justice, Guidance on Coordinating Corporate Resolution Penalties in Parallel Criminal, Civil, Regulatory, and Administrative Proceedings (June 5, 2025), https://www.justice.gov/criminal/media/1402751/dl.

[8]Economic Crime and Corporate Transparency Act 2023, c. 56 (UK).

[9]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199(1) (UK).

[10]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199(1) (UK).

[11]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199(4) (UK).

[12]UK Home Office, Economic Crime and Corporate Transparency Act 2023: Guidance to organizations on the offense of failure to prevent fraud (accessible) ch. 3 (updated Oct. 10, 2025), https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version.

[13]UK Home Office, Economic Crime and Corporate Transparency Act 2023: Guidance to organizations on the offense of failure to prevent fraud (accessible) § 2.5 (updated Oct.10, 2025), https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version.

[14]31 U.S.C.A. § 3729.

[15]See False Claims Amendments Act of 1986, Pub. L. No. 99-562, 100 Stat. 3153 (1986) (codified as amended at 31 U.S.C.A. §§ 3729–3733).

[16]31 U.S.C.A. § 3730.

[17]Press Release, U.S. Dep't of Justice, False Claims Act Settlements and Judgments Exceed $2.9B in Fiscal Year 2024, justice.gov (Jan. 15, 2025), https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024.

[18]U.S. Dep't of Justice, Justice Manual § 4-4.112, Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters (May 2019).

[19]Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa A. 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.

[20]Economic Crime and Corporate Transparency Act 2023, c. 56, § 201 (UK).

[21]Economic Crime and Corporate Transparency Act 2023, c. 56, § 201(1) (UK).

[22]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199(2) (UK).

[23]31 U.S.C.A. § 3729.

[24]Economic Crime and Corporate Transparency Act 2023, c. 56, Sch. 13 (UK).

[25]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199(1) (UK).

[26]31 U.S.C.A. § 3729.

[27]31 U.S.C.A. § 3729(b)(2).

[28]E.g., Press Release, U.S. Dep't of Justice, Health Net Federal Services, LLC and Centene Corporation

Agree To Pay Over $11 Million To Resolve False Claims Act Liability for Cybersecurity Violations (Feb. 18, 2025), https://www.justice.gov/opa/pr/health-net-federal-services-llc-and-centene-corporation-agree-pay-over-11-million-resolve.

[29]E.g., Press Release, U.S. Dep't of Justice, Connecticut Company and Owner Settle Liability for False Claims Related to Violations of Buy American Act and Trade Agreements Act (May 20, 2025), https://www.justice.gov/usao-ct/pr/connecticut-company-and-owner-settle-liability-false-claims-related-violations-buy.

[30]E.g., Press Release, U.S. Dep't of Justice, Vohra Wound Physicians and its Owner Agree To Pay $45 Million To Settle Fraud Allegations of Overbilling for Wound Care Services (Nov. 21, 2025), https://www.justice.gov/opa/pr/vohra-wound-physicians-and-its-owner-agree-pay-45m-settle-fraud-allegations-overbilling.

[31]E.g., Press Release, U.S. Dep't of Justice, Florida Businessman Patrick Walsh and Affiliated Companies Agree to $20M Consent Judgment To Settle False Claims Act Liability Relating to Fraudulent Pandemic Relief Loans (Mar. 12, 2025), https://www.justice.gov/opa/pr/florida-businessman-patrick-walsh-and-affiliated-companies-agree-20m-consent-judgment-settle.

[32] Universal Health Servs., Inc. v. United States ex rel. Escobar, 579 U.S. 176, 190 (2016).

[33]31 U.S.C.A. § 3729.

[34]UK Home Office, Economic Crime and Corporate Transparency Act 2023: Guidance to organizations on the offense of failure to prevent fraud (accessible) § 2.5 (updated Oct.10, 2025), https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version.

[35]Economic Crime and Corporate Transparency Act 2023, c. 56, § 199(4) (UK).

[36]UK Home Office, Economic Crime and Corporate Transparency Act 2023: Guidance to organizations on the offense of failure to prevent fraud (accessible) ch. 3 (updated Oct.10, 2025), https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version.

[37]UK Ministry of Justice, Guidance on The Bribery Act 2010 (Mar. 2011), https://www.gov.uk/government/publications/bribery-act-2010-guidance.

[38]On November 26, 2025 the UK Serious Fraud Office (SFO) published its first ever guidance on Evaluating Corporate Compliance Programmes. The document provides organizations with greater visibility into how the SFO assesses the effectiveness of compliance programmes and how those assessments influence decisions on prosecution, Deferred Prosecution Agreements (DPAs), statutory defenses and sentencing. UK Serious Fraud Office, Guidance on Evaluating a Corporate Compliance Programme (Nov. 26, 2025), https://www.gov.uk/government/publications/sfo-guidance-on-evaluating-a-corporate-compliance-programme/sfo-guidance-on-evaluating-a-corporate-compliance-programme.

[39]31 U.S.C.A. § 3730.

[40]Press Release, U.S. Dep't of Justice, False Claims Act Settlements and Judgments Exceed $2.9B in Fiscal Year 2024, justice.gov (Jan. 15, 2025), https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024.

[41]31 U.S.C.A. § 3729(a).

[42]FAR 9.406-2.

[43]U.S. Dep't of Justice, Justice Manual 4-4.112, Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters (May 2019).

[44]Deputy Attorney General Lisa A. 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.

[45]False Claims Act Settlements and Judgements Exceed $2.9B in Fiscal Year 2024 (Jan. 15, 2025), https://www.justice.gov/archives/opa/pr/false-claims-act-settlements-and-judgments-exceed-29b-fiscal-year-2024.

[46]U.S. Dep't of Justice, Corporate Whistleblower Awards Pilot Program Guidance (issued Aug. 1, 2024; revised May 12, 2025), https://www.justice.gov/criminal/media/1400041/dl?inline.

[47]HM Revenue & Customs, Reporting Serious Tax Avoidance or Evasion (updated Nov. 26, 2025), https://www.gov.uk/guidance/reporting-serious-tax-avoidance-or-evasion.

[48]HM Revenue & Customs, Reporting Serious Tax Avoidance or Evasion (updated Nov. 26, 2025), https://www.gov.uk/guidance/reporting-serious-tax-avoidance-or-evasion; see U.S. Internal Revenue Service, Whistleblower Office (updated Oct. 17, 2025), https://www.irs.gov/compliance/whistleblower-office.

[49]UK Serious Fraud Office, Serious Fraud Office Strategy 2024–2029, at 10 (Apr. 18, 2024), https://www.sfo.gov.uk/about-us/strategy/; U.S. Dep't of Justice, Corporate Whistleblower Awards Pilot Program Guidance (issued Aug. 1, 2024; revised May 12, 2025), https://www.justice.gov/criminal/media/1400041/dl?inline.

[50]While the focus of this article is on the civil FCA, there is a criminal corollary (18 U.S.C.A. § 287) with a different level of intent and burden of proof than the civil FCA. Additionally, only the DOJ can bring a criminal FCA case, while the civil FCA contains *qui tam* provisions.

NOTES:

NOTES:

BRIEFING PAPERS