King & Spalding

Client Alert

Special Matters & Government Investigations

DECEMBER 02, 2024

For more information, contact:

Aaron Stephens
+44 20 7551 2179
astephens@kslaw.com

Max Benjamin Hill, K.C.
+44 20 7551 2130
mhill@kslaw.com

Margaret Nettesheim
+44 20 7551 7592
mnettesheim@kslaw.com

Alexander Tivey (Alex)
+44 20 7551 7577
ativey@kslaw.com

King & Spalding

London
8 Bishopsgate
London, EC2N 4BQ
United Kingdom
T. +44 20 7551 7500

The 'Failure to Prevent Fraud' Offence: A Phased Approach to Implementing Effective Fraud Prevention Procedures

INTRODUCTION

The Economic Crime and Corporate Transparency Act 2023 (the "**ECCTA**") introduced a corporate 'failure to prevent fraud' offence providing that 'large' organisations may be held criminally liable if an 'associate' (such as an employee, agent, or subsidiary) commits a specified fraud offence[i] intended to benefit the organisation or its clients.[ii] The failure to prevent fraud offence requires a specific UK nexus – i.e., one of the acts which was part of the base fraud offence must take place in the UK, or the gain or loss must occur in the UK.[iii] This requirement distinguishes the 'failure to prevent fraud' offence from the 'failure to prevent bribery' offence under the UK Bribery Act 2010 (the "**UKBA**"), which applies to UK-incorporated commercial organisations and non-UK companies that carry on business (or part of a business) in the UK, irrespective of where the bribery occurs.[iv]

'Failure to prevent fraud' is a strict liability offence; there is no requirement to demonstrate that the organisation's senior managers/directors knew about the fraud in order to hold the organisation criminally liable. However, similar to the UKBA, there is a statutory defence where an organisation can demonstrate either that it had reasonable procedures in place to prevent fraud, or that it was not reasonable in the circumstances to expect it to have any prevention procedures in place.[v]

On 6 November 2024, the UK Home Office published statutory guidance on the 'failure to prevent fraud' offence (the "**Guidance**") and, of particular note, what will be considered reasonable fraud prevention procedures to satisfy the requirements of the statutory defence.[vi] The offence comes into effect nine months from the publication of the

Guidance, or 1 September 2025.[vii] This article recommends near-, medium-, and long-term steps which in-scope organisations should take to ensure they have reasonable fraud prevention procedures in place to guard against liability for breaches of the 'failure to prevent fraud' offence.

IN-SCOPE ORGANISATIONS

The 'failure to prevent fraud' offence applies to 'large organisations.' A 'large organisation' is one which meets at least two of the following three criteria in the financial year preceding the fraud offence (or which is a subsidiary of an organisation that meets the same criteria):

i. turnover of more than £36 million (£36 million net or £43.2 million gross for parent undertakings);

ii. total assets of more than £18 million (£18 million net or £21.6 million gross for parent undertakings);

iii. more than 250 employees.

FRAUD PREVENTION GUIDANCE

The Guidance describes six key principles which organisations should consider when implementing reasonable fraud prevention measures:

- top level commitment;
- risk assessment;
- proportionate risk-based prevention procedures;
- due diligence;
- communication (including training); and
- monitoring and review.[viii]

Ultimately, what will be considered 'reasonable' and how best to apply these principles will depend on an organisation's risk profile and its activities. In-scope organisations must take thoughtful action to implement or update fraud prevention procedures in accordance with the Guidance before the offence comes into effect in September 2025 and plan for ongoing risk mitigation strategies thereafter.

NEAR-TERM ACTIONS

As soon as possible, in-scope organisations, with the assistance of outside counsel where necessary, should take the following steps to kickstart their review and implementation of fraud prevention procedures:

1. Assign oversight responsibility for fraud prevention programmes to the relevant compliance or legal personnel, both in the parent organisation and any subsidiaries. It is important to ensure that the appointed personnel have the necessary qualifications and sufficient capacity to devote meaningful attention to fraud prevention. If necessary, hire additional support.

2. Conduct a fraud-focused risk assessment to identify applicable 'typologies of risk' by examining ways in which the business model creates or allows for opportunity, motive, and rationalisation for fraud.[ix] For example, incentive-based compensation for sales personnel dependent on meeting sales targets coupled with inadequate oversight and a sense that the targets are unreasonable could create the opportunity and motivation for sales personnel to defraud customers to inflate their sales numbers and then rationalise their actions to themselves. It may make sense to engage forensic accountants to assist with this process. The risk assessment should also include an examination of territoriality, subsidiaries, and supply chain issues.

For example, if a foreign agent of an in-scope organisation engaged in manufacturing commits fraud in sourcing raw materials for that organisation (such that the in-scope organisation pays less for the materials to the detriment of the suppliers) the organisation would arguably be on the hook for failing to prevent fraud because the gain occurred in the UK. The risk assessment should look critically at commercial supply chains to ascertain where extraterritorial activity could nonetheless give rise to a failure to prevent fraud charge because there is an impact in the UK.

3. Identify any other laws or regulations already applicable to the organisation which have compliance requirements which will overlap with fraud prevention procedures. For example, consider whether the organisation is subject to (or likely to be caught by) the failure to prevent the facilitation of tax evasion offence in the Criminal Finances Act 2017, auditing requirements under s.475 of the Companies Act 2006 and/or the Financial Reporting Council's UK auditing standard (ISA (UK) 240), or the risk assessment requirements for premium listed companies under the UK Corporate Governance Code. 'Adequate procedures' developed and maintained in relation to the UKBA may also have some overlap with fraud prevention procedures. Avoid duplication where existing policies and procedures in place to address such regulations also cover off elements of fraud prevention and ensure that new fraud prevention procedures sync up with existing policies and procedures.
4. Conduct management briefings on the new offence and the importance of implementing adequate fraud prevention procedures. These briefings will begin the process of setting a 'tone at the top' which prioritises an anti-fraud culture and cascading that message down to mid-level managers and staff.

MEDIUM-TERM ACTIONS

Once the near-term actions have been completed and before September 2025, in-scope organisations should do the following, again with the assistance of outside counsel as needed:

1. If additional compliance or legal personnel need to be hired to implement and enforce fraud prevention procedures, initiate the recruitment process with a view toward hiring the necessary personnel by the summer to enable them to get up to speed by September.
2. Conduct a gap analysis of existing compliance policies and procedures against fraud risks identified in the risk assessment to identify where additional policies are required or where existing policies such as codes of conduct, codes of ethics, conflicts of interest policies, and whistleblowing procedures need to be expanded in order to create an adequate fraud prevention plan proportionate to the fraud risks the organisation faces.[x] Draft or revise policies accordingly. Additionally, consider implementing practical rules to help prevent fraud, such as prohibiting employees from using off-channel communications (e.g., personal mobile devices, WhatsApp, iMessage, Signal, Telegram) for business purposes, and/or rolling out an enterprise-wide messaging solution to enable staff to use these types of platforms in a way that can be monitored and preserved by the company.[xi]
3. Update processes for transactional and third party risk management due diligence to include an evaluation of fraud risk. Ensure that any technological screening tools used will pick up fraud risk factors such as related party transactions, sham entities, or prior legal claims relating to alleged fraud, or consider the implementation of such tools if the organisation is not already using them and conducts diligence on a large volume of parties. Additionally, conduct due diligence on existing 'associated persons' relationships to identify any areas of fraud risk. In particular, due diligence should be conducted on sales agents, representatives and other entities or individuals that provide services for or on behalf of (but not to) the organisation. Where an organisation has a sizeable number of 'associated persons' relationships, consider

applying a risk rating (which may take into account the location of the associated person, the type of work they do for the organisation, and the financial value of the organisation's contract with them) to triage the diligence by magnitude of fraud risk.

4. Update template supplier and third party service provider (together, "**third parties**") contracts to include fraud prevention clauses and use a revised template for all new third party relationships going forward. For example, organisations may wish to introduce clauses prohibiting certain acts (such as committing any of the fraud offences specified in the ECCTA) and ensuring third party compliance with relevant fraud-related legislation (including, but not limited to, the ECCTA), along with related warranties and indemnities. Organisations may also wish to require third parties to comply with the organisation's fraud prevention policies and provide annual compliance certifications. Ensure that any such fraud prevention clauses include a requirement for third parties to introduce equivalent provisions in their own contracts with subcontractors and representatives engaged for the work the third party is providing to the organisation.
5. Begin the process of exiting relationships with third parties that present unacceptable levels of fraud risk, complying with the termination clauses in their contracts, which may require a written notification and impose a notice period or other obligations.
6. Develop an employee training programme relating to the failure to prevent fraud offence and conduct initial training to ensure that prevention policies and procedures are adequately communicated, embedded, and understood throughout the organisation. Initial training should include an overview of changes to existing policies as well as any new policies and should note the consequences and internal disciplinary process for those found to have committed fraud. Organisations may wish to provide similar training to their third parties, particularly where third party relationships present significant risk. The initial training should also ensure that employees and third parties are familiar with the organisation's whistleblowing policy and procedures. Consider whether specialised training for particularly exposed employees (including employees carrying out third party due diligence), or third parties themselves, is necessary and develop focused training if so.

LONG-TERM ACTIONS

The below are additional actions organisations should take on a longer-term and/or ongoing basis:

1. Consider changes to compensation and incentive structures or other aspects of the organisation's business model to reduce specific 'typologies of risk' identified in the risk assessment.
2. Conduct testing of the fraud prevention procedures to ensure their effectiveness. Specific guidance on testing fraud controls is available for public companies,[xii] whereas private sector organisations have more flexibility to choose how to test their fraud prevention measures. Testing may entail observing how the fraud prevention procedures are applied (via a system or process walkthrough, or workshops with stakeholders), analysing how they function (through sample reviews or data analysis), and actively pressure testing how they operate (through technical or covert testing to breach controls). Such testing should be conducted by members of the organisation who were not involved in developing the procedures. Once testing has taken place, any issues or residual risks identified should be assessed and, if necessary, addressed with further, specific fraud prevention measures.
3. Conduct annual or biannual fraud risk assessments. If applicable, roll these risk assessments into any existing, enterprise-wide risk assessment schedule. Consider whether various external factors or events (such as a whistleblower report or fraud investigation, or a fundraising campaign or impending transaction involving the organisation) should trigger an earlier or interim review.

4. Conduct employee/third party training at a regular cadence and update employees/third parties on the outcomes of fraud-related investigations. Employee training programmes should be regularly reviewed and updated to reflect any changes to the law or lessons learned from fraud issues that arise over time.
5. Renegotiate third party contracts at renewal dates to incorporate fraud prevention clauses. These clauses should be based on the revised template referenced above.
6. Implement a range of measures, such as technological solutions and analytical tools, to monitoring for fraud. For example, consider what analysis the organisation currently carries out of the procurement process, incoming and outgoing invoices, and incoming and outgoing payments, how discrepancies or indications of suspicious activity are flagged and to whom, and whether this process can be automated.
7. Investigate instances of suspected fraud. Investigations should be independent, clear about their internal client and purpose, appropriately resourced and scoped, and legally compliant. Organisations should ensure that any investigation is conducted either by in-house or outside counsel, as opposed to non-lawyer personnel, to ensure it attracts legal professional privilege.

---

[i] i.e., one of the offences specified in Schedule 13 to the Act or the aiding, abetting, counselling, or procuring of such an offence; https://www.legislation.gov.uk/ukpga/2023/56/schedule/13/enacted.
[ii] https://www.legislation.gov.uk/ukpga/2023/56/section/199.
[iii] The Guidance, §2.5.
[iv] https://www.legislation.gov.uk/ukpga/2010/23/crossheading/failure-of-commercial-organisations-to-prevent-bribery; https://www.legislation.gov.uk/ukpga/2010/23/section/12.
[v] For more information on the failure to prevent fraud offence and the ECCTA more generally, see our New Law Journal article entitled 'Corporate Criminal Liability: A Wider Scope?', https://www.newlawjournal.co.uk/content/corporate-criminal-liability-a-wider-scope-.
[vi] 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.
[vii] The Guidance, §1.3.
[viii] The Guidance, §3.
[ix] For more on 'typologies of risk', see the Guidance, §3.2.
[x] The Guidance, §3.3.
[xi] For more on off-channel communications, see our Client Alert entitled 'Recent Enforcement Trends Regarding the Use of Off-Channel Communications on Personal Devices', https://www.kslaw.com/news-and-insights/recent-enforcement-trends-regarding-the-use-of-off-channel-communications-on-personal-devices.
[xii] https://www.gov.uk/government/publications/international-public-sector-fraud-forum-guidance.

Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

J.C. Boggs
Washington, DC
+1 202 626 2383
jboggs@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
Washington, DC
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Ander M. Crenshaw
Washington, DC
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Ethan P. Davis
San Francisco
+1 415 318 1228
edavis@kslaw.com

Alan R. Dial
Washington, DC
+1 202 661 7977
adial@kslaw.com

Dan Donovan
Washington, DC
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
Washington, DC
+1 202 626 9710
rehrlich@kslaw.com

David Farber
Washington, DC
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Emily Gordy
Washington, DC
+1 202 626 8974
egordy@kslaw.com

Leah B. Grossi
Washington, DC
+1 202 626 5511
lgrossi@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Zachary J. Harmon
Washington, DC
+1 202 626 5594
zharmon@kslaw.com

Ted Hester
Washington, DC
+1 202 626 2901
thester@kslaw.com

Max Hill, K.C.
London
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Rob Hur
Washington, DC
+1 202 383 8969
rhur@kslaw.com

Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

Barry Kamar
Miami
+1 305 462 6044
bkamar@kslaw.com

Allison F. Kassir
Washington, DC
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
Washington, DC
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
Washington, DC
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
Atlanta
+1 404 572 2747
amedina@kslaw.com

Kendrick B. Meek
Washington, DC
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Jim C. Miller III
Washington, DC
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
Washington, DC
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
Miami
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Anthony A. Williams
Washington, DC
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com