

GIBSON DUNN



White Collar Defense & Investigations Update

November 6, 2024

## Publication of UK Government Guidance on Failure to Prevent Fraud Offence

The much-anticipated guidance for the new corporate offence of failure to prevent fraud (the “Guidance”) was published on 6 November 2024. This starts the countdown to the offence coming into force on 1 September 2025.<sup>[1]</sup>

Introducing a “*failure to prevent*” offence for fraud will have a significant impact on the ability of law enforcement agencies to combat fraud. The SFO said it is “*looking forward to using it to penalise large organisations who should be doing better*”<sup>[2]</sup> and the SFO’s Director, Nick Ephgrave, recently told the Financial Times that deferred prosecution agreements (DPAs) “*could come back with a vengeance once a new offence that puts the onus on businesses to prevent fraud comes into force.*”<sup>[3]</sup> The Guidance itself mentions the prospect of DPAs.

The Guidance states that the failure to prevent fraud offence should make it easier to hold organisations to account. The Government hopes that the offence will improve fraud prevention procedures and ultimately drive a major shift in corporate culture.<sup>[4]</sup>

### A) Recap of the failure to prevent fraud offence

The offence of failure to prevent fraud was introduced by the Economic Crime and Corporate Transparency Act 2023 (ECCTA).<sup>[5]</sup> Under the new offence, an organisation will be criminally liable<sup>[6]</sup> where a specified fraud offence<sup>[7]</sup> is committed by a person associated with the organisation (such as an employee or agent) with the intention of benefitting, for example, the organisation or its clients. Senior managers need not have ordered or known about the fraud.

The offence applies to large organisations, which are those meeting at least two of the following conditions: a turnover of more than £36m, more than £18m in total assets, or more than 250 employees.<sup>[8]</sup> A defence is available where an organisation had reasonable prevention procedures in place, or where it was unreasonable to expect it to have such procedures.

## **B) What does the Guidance say?**

The Guidance offers clarification of certain aspects of the offence in section 199 ECCTA, provides examples of hypothetical scenarios in which the offence may apply and makes recommendations as to how companies should prepare for the new offence coming into force. However, it remains to be seen how the offence will be prosecuted in practice. We have outlined key aspects of the Guidance below.

### **1. Territoriality**

ECCTA states that the failure to prevent fraud offence applies to organisations wherever incorporated or formed.<sup>[9]</sup> However, a UK nexus is required for the offence to be committed, which means “one of the acts which was part of the underlying fraud took place in the UK or that the gain or loss occurred in the UK.”<sup>[10]</sup> The Guidance indicates that this means that a fraud which takes place entirely outside the UK could be prosecuted if, for example, there were UK-based victims.

### **2. Offences committed by associated persons**

The concept of a *person associated* with an organisation will be familiar from the UK Bribery Act. The Guidance confirms that an employee, agent or subsidiary of a large organisation automatically falls within the definition of *associated person*, and a person who provides services *for or on behalf of the organisation* is an *associated person* while they provide those services.<sup>[11]</sup>

Crucially, the associated person does not need to have been convicted of one of these offences. However, the prosecution must prove to a criminal standard that the person committed the offence before the organisation can be convicted of failure to prevent fraud.<sup>[12]</sup>

### **3. Subsidiaries**

In respect of *subsidiaries*, the guidance indicates that:

- a large organisation can be prosecuted where the underlying offence is committed corporately by one of its subsidiaries and where the beneficiary is the parent organisation or its clients to whom the subsidiary provides services for or on behalf of the parent;
- such a parent company can also be prosecuted if an employee of its subsidiary commits a relevant offence that is intended to benefit the parent company;
- a subsidiary of a large organisation can be prosecuted if an employee of the subsidiary commits a relevant offence that is intended to benefit the subsidiary even if the subsidiary itself is not a large organisation.<sup>[13]</sup>

## 4. Benefit

The issue of who is intended to benefit from the underlying offence is key to determining whether a company can be held accountable.<sup>[14]</sup> The benefit can be direct or indirect, actual or intended.<sup>[15]</sup> The benefit can be to the company, its clients, or a subsidiary of the client.<sup>[16]</sup> This is broader than the UK Bribery Act, which focuses on intended benefit to the organisation.

## 5. What do reasonable fraud prevention procedures look like in practice?

The defence of having reasonable fraud prevention measures in place is difficult to define, and the Guidance does not attempt to set out an exhaustive list of steps that companies should take: in fact, it notes expressly that even strict compliance with the Guidance may not be sufficient where a company faces particular risks arising from the nature of its business.

Nevertheless, the Guidance does set out six defining principles which should inform a company's fraud prevention framework. Some key points are highlighted below:

### 1. Top level commitment

- The Guidance stresses that **senior management should take the lead** when it comes to fraud prevention: this will include fostering a culture in which staff feel able to report potential cases of fraud, and communicating clearly the company's policies and codes of practices to staff.
- Where fraud prevention measures are overseen by a Head of Compliance or someone in a similar role, that person should have **direct access to the company's board or CEO**, and senior management should ensure that a **reasonable and proportionate budget** is in place to train staff and implement the company's fraud prevention plan.

### 2. Risk assessment

- The Guidance makes clear that "*it will rarely be considered reasonable not to have even conducted a risk assessment*" but it acknowledges that companies may find it most effective to **extend existing risk assessments** which are already in place.
- The Guidance suggests that companies should consider the **different levels of fraud risk presented by different categories of associated person**, taking into account their opportunity and motive to commit fraud, as well as the potential for the "*rationalisation*" of a fraud: in other words, does a company's culture and/or sector tolerate fraud, and do staff feel able to escalate any potential concerns?
- **A risk assessment is not a one-off exercise**: the Guidance states that the assessment should be revisited at consistent intervals, perhaps annually or bi-annually, and that a court may consider that reasonable procedures were not in place at the time of any alleged fraud if the risk assessment has not been recently reviewed.

### 3. Proportionate risk-based prevention procedures

- Once the risk assessment has been carried out, a **fraud prevention plan** should be put in place. This should be proportionate to the risks identified and their potential impact.

- **Reasonable fraud prevention procedures** should look to **reduce the opportunity and motive to commit fraud**, put in place consequences for committing fraud and reduce what the Guidance describes as “*ethical fading*”; in other words, where fraudulent behaviour becomes normalised within a company or industry.
- The Guidance acknowledges that many companies will be regulated, but stresses that **processes and procedures already in place** to ensure compliance with other regulations **will not automatically qualify as reasonable procedures** for the purposes of ECCTA.
- One interesting exception identified in the Guidance, presumably inspired by lessons from the Covid-19 pandemic, is where there is an emergency; i.e. where there is “*a risk of widespread loss of life or damage to property, or significant financial instability*”. The Guidance recognises that an **emergency may not be foreseeable**, and that it **may therefore be reasonable not to have had fraud prevention procedures** in place. Nevertheless, the guidance stresses that reasonable procedures should be put in place as quickly as reasonably possible once the emergency has passed.

#### 4. Due diligence

- Again, the Guidance acknowledges that many companies will already have due diligence procedures in place, but states that it will **not necessarily be sufficient to apply existing procedures**.
- The Guidance highlights the need to carry out due diligence on associated persons and in relation to any anticipated mergers or acquisitions. It suggests **using appropriate technology** to help, including third-party tools, and notes the importance of integrating existing fraud prevention measures following a merger or acquisition.

#### 5. Communication and training

- **Clear communication** of a company’s stance on fraud **at all levels of the organisation** is important, and the Guidance suggests incorporating this in existing policies.
- Companies should put in place **training for staff which is proportionate to the risks** involved. That may involve additional training for those in high-risk positions. As with the risk assessment, training should be kept up to date, particularly as new staff join or existing staff change roles, and the effectiveness of the training should be monitored.
- The Guidance also highlights the need for a **robust whistleblowing process**.

#### 6. Monitoring and review

- When it comes to **detecting fraud**, the Guidance again highlights the **use of technology** such as **data analytics tools**, and poses the question (but does not answer it!) as to whether **AI could be used to identify potential fraud**.
- Companies may need to modify existing systems to identify and investigate fraud committed against the organisation to ensure that fraud designed to benefit the organisation or its clients can also be detected.
- The Guidance stresses the **need for independent, fair, legally compliant and properly resourced investigations** into any suspected fraud.

- A company will need to **keep under review the nature of the risks it faces**, given these are likely to change over time: this means **fraud prevention measures may need to change** too. The Guidance suggests that reviews should happen at **regular intervals**, such as annually or bi-annually, and that they can be conducted internally or by an external party.
- However, where a company is audited by an external auditor, that audit alone is not sufficient evidence of the existence of reasonable fraud prevention

### C) Practical steps to take now

By way of key takeaways, we recommend that clients think about the following next steps:

- ***Conduct a risk assessment for the organisation as a whole. It is clear that this is the minimum first step towards having reasonable fraud prevention procedures in place and, given the scope of the different definitions in ECCTA, is likely to require revision or development of existing assessments;***
- ***Establish a reasonable and proportionate fraud prevention plan;***
- ***Review existing policies and procedures and ensure that the company's stance of preventing fraud is clearly communicated to staff;***
- ***Check what training is currently provided to staff and consider where additional training on preventing fraud could be necessary;***
- ***Ensure that robust whistleblowing policies and procedures are in place;***
- ***Where in doubt, seek expert advice.***

[1] <https://www.gov.uk/government/news/new-failure-to-prevent-fraud-guidance-published>

[2] <https://globalinvestigationsreview.com/article/senior-sfo-lawyer-failure-prevent-fraud-heralds-exciting-time-the-agency>

[3] <https://www.ft.com/content/b7540e7a-97fb-481a-8805-92fb54a425f2>

[4] Guidance Failure to Prevent Fraud, chapter 1.1. See also our previous client alert published on 12 January 2024: [Extraterritorial Impact of New UK Corporate Criminal Liability Laws - Gibson Dunn](#)

[5] ECCTA s.199

[6] ECCTA s.199 and Guidance Failure to Prevent Fraud, chapter 1.1

[7] Including fraud by false representation, fraud by failing to disclose information, fraud by abuse of position, cheating the public revenue, false accounting, false statements by company directors and fraudulent trading: see ECCTA, schedule 13.

[8] ECCTA s.201. The conditions must be met in the financial year of the organisation that precedes the year of the fraud offence.

[9] ECCTA s.199(13)

[10] Guidance Failure to Prevent Fraud chapter 2.5

[11] ECCTA s.199 (7) and (8) and Guidance Failure to Prevent Fraud chapter 2.3

[12] Guidance Failure to Prevent Fraud chapter 2.2

[13] Guidance Failure to Prevent Fraud chapter 2.3.1 and ECCTA s.199

[14] Guidance Failure to Prevent Fraud chapter 2.4

[15] ECCTA s.199 (1) and (2)

[16] Guidance Failure to Prevent Fraud chapter 2.4 and 2.5

**The following Gibson Dunn lawyers prepared this update: Allan Neil, Patrick Doris, Christopher Loudon, Marija Bračković, Amy Cooke, and Katherine Tomsett.**

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. If you wish to discuss any of the matters set out above, please contact the Gibson Dunn lawyer with whom you usually work, any leader or member of Gibson Dunn's White Collar Defense and Investigations practice group, or the authors:

Allan Neil – London (+44 20 7071 4296, [aneil@gibsondunn.com](mailto:aneil@gibsondunn.com))

Patrick Doris – London (+44 20 7071 4276, [pdoris@gibsondunn.com](mailto:pdoris@gibsondunn.com))

Christopher Loudon – London (+44 20 7071 4249, [cloudon@gibsondunn.com](mailto:cloudon@gibsondunn.com))

Marija Bračković – London (+44 20 7071 4143 [mbrackovic@gibsondunn.com](mailto:mbrackovic@gibsondunn.com))

Amy Cooke – London (+44 20 7071 4041, [acooke@gibsondunn.com](mailto:acooke@gibsondunn.com))

Katherine Tomsett – Hong Kong (+65 6507 3673, [ktomsett@gibsondunn.com](mailto:ktomsett@gibsondunn.com))

Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client

relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

If you would prefer NOT to receive future emailings such as this from the firm, please reply to this email with "Unsubscribe" in the subject line.

If you would prefer to be removed from ALL of our email lists, please reply to this email with "Unsubscribe All" in the subject line. Thank you.

© 2024 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at [gibsondunn.com](https://www.gibsondunn.com)