# Mountains and molehills: does new government fraud guidance help companies tell the difference?

⋮ 12/11/2024

Last week, the government released guidance on the new offence of failure to prevent (FTP) fraud. In the first of a series of four articles, we analyse what companies and their advisers need to know about this significant development.

“Reasonable” and “proportionate”: these important terms form the basis of new government guidance on the fraud prevention procedures that many companies will need to implement to mitigate the risk of criminal liability. Do they provide a clear and practical roadmap to compliance, or will their imprecision lead companies to slip up? The government will argue they are the former, although the guidance itself suggests that the Serious Fraud Offence (SFO) is banking on the latter.

**What does the guidance cover?**

The guidance was published to advise organisations on the new offence of FTP fraud and the associated “reasonable procedures” defence, which will come into force on 1 September 2025.

The new offence, which applies to “large organisations”[1] and their subsidiaries, is committed if someone associated with the organisation – such as an employee, agent or person providing services on its behalf – commits fraud with the intention of benefiting the organisation or its clients. However, the organisation will have a complete defence if it can demonstrate that it “had in place such prevention procedures as it was reasonable in all the circumstances to expect the body to have in place”. The bulk of the guidance contains advice as to what “prevention procedures” will be considered “reasonable” and therefore will constitute a defence.

The guidance claims to be “flexible and outcome focussed” but, in fact, is remarkably prescriptive, with six principles for reasonable fraud prevention procedures broken down over 16 pages. However, what companies will want to know most is how the “reasonable procedure” standard will apply to their specific circumstances, depending for example, on their size, structure, market conditions and industry sector.

Despite the glut of advice – there are 115 specific, bulleted suggestions for best practice – there is scant detail about how the “reasonable procedures” standard will be applied differentially in practice.

The guidance acknowledges the lack of detail and alludes to a proposed solution, namely that companies read the public documents to be released following any prosecution or deferred prosecution agreement (DPA) made under the new offence. This risks creating an unfair and uncertain state of affairs for organisations.

The result is that the government has written guidance about “reasonable procedures” which tells us that the meaning of “reasonable procedures” will be revealed only when the SFO brings a prosecution based on what it thinks “reasonable procedures” means, and a court then decides whether the SFO were right. In other words, to find out how many of the 115 bullets points it will be reasonable and proportionate to follow, companies will have to wait for others to fail.

This disjunction between deterrence and prosecution pervades the guidance. The government wants organisations to bear the brunt of the cost and responsibility for preventing corporate fraud, and companies now have nine months to develop and implement fraud prevention procedures before the offence comes into force in September 2025. But, the SFO does not want the guidance to be too helpful, which might inhibit prosecutions. This leaves the burden on companies and their advisers to work out what the SFO and, ultimately, a court might consider reasonable and proportionate in the circumstances. Such uncertainty is likely to lead to an overly cautious approach until and unless future prosecutions allow for finer calibrations of risk.

**Some practical information**

These problems aside, the guidance contains plenty of helpful and practical information about fraud prevention.

The chapter on reasonable fraud prevention procedures is broadly similar to equivalent guidance introduced for the FTP bribery offence and FTP tax evasion offences in 2011 and 2017, respectively. As such, the FTP fraud offence guidance uses a familiar set of six principles designed to inform an organisation’s fraud prevention framework, although with some differences in emphasis.

*Top level commitment*

The first principle gives specific and notable reference to “senior management” being part of compliance leadership within an organisation. This makes the definition of “top level commitment” deliberately broader than in previous guidance which referred only to the “board of directors” and “owners”.

*Risk assessment*

The second principle in the guidance suggests that the minimum standard – and starting point – for a reasonable fraud prevention procedure is a relevant and documented risk assessment; it will be rarely considered reasonable not to have one.

*Proportionate procedures*

The third principle is largely redundant. One purpose it does serve though, is to make it clear that there are no existing shortcuts to compliance, even for regulated companies: compliance processes under existing regulations do not automatically qualify as “reasonable procedures”, and audited companies cannot rely solely on the audit to provide them with assurance.

*Due diligence*

The fourth principle refers specifically to best practice in due diligence during mergers and acquisitions. This is noteworthy because it highlights the type of companies that are most likely to come unstuck by the

new offence: those that have recently undergone a significant change in structure, management, ownership or financing. Indeed, a company that finds itself growing at a fast rate due to being recently acquired or having recently received large investment or financing is less likely to have a compliance framework which is proportionate to its new size.

*Communication*

On its face, the fifth principle tells organisations to embed their prevention procedures into their workforce via internal and external communication. More interestingly however, is the specific section dedicated to whistleblowing. The FTP fraud guidance mentions whistleblowing far more (34 times) than either the FTP bribery (twice) or FTP tax evasion (seven times) guidance. The emphasis placed on whistleblowing suggests, for at least the short-medium term, that it should be a key component of the compliance procedures of relevant organisations.

This shift in emphasis appears to reflect the changing belief of regulators and the government that whistleblowing could be used far more effectively. For example, the director of the SFO, Nick Ephgrave, raised eyebrows earlier this year with his bold suggestion that the US system of rewarding whistleblowing should be implemented in the UK.

*Monitoring and review*

It is unremarkable that the government believes that organisations should monitor and review their fraud prevention procedures on an ongoing basis. More remarkable is the suggested methods of doing so. For this, the guidance suggests technology solutions such as data analytics and artificial intelligence. In fact, four of the six principles in the guidance recommend the use of these technology solutions to implement fraud prevention procedures.

This gives much greater emphasis to the role of technology in compliance than provided in previous guidance. The use of technology raises the possibility that organisations outsource their compliance functions to software or to third parties. It is unclear what level of oversight would be considered “reasonable” in such arrangements. The emphasis on technology in the guidance should also demonstrate the importance of incorporating an organisation’s IT function into its compliance framework.

**Potential vectors of enforcement**

Finally, some very important takeaways from the guidance are the fact patterns that are likely to prompt enforcement of the new offence. In eight hypothetical case studies, the guidance highlights ESG fraud and the extra-territorial reach of the offence as potential vectors of enforcement.

To explain these scenarios in more depth, and to reveal the future effects of the guidance and new offence, this article will be followed in the next few weeks by three others. In sequence, these articles will: explain how ESG fraud could be prosecuted under the new offence, reveal how overseas companies could be prosecuted under the offence’s extra-territorial scope, and explore what the future effect of the new FTP fraud offence and guidance is likely to be.

**Footnote**

[1] Large organisations are defined by relevant legislation as an entity satisfying two of the following three criteria: more than 250 employees; more than £36 million turnover; or more than £18 million total assets.