Linklaters

Nine months and counting: The government publishes its guidance on the new failure to prevent fraud offence

07 November 2024

Contents

The long-awaited guidance for organisations on the new failure to prevent fraud offence was published on 6 November 2024. It paves the way for the latest in the "failure to prevent" offences to come into effect – in-scope organisations should start to prepare now for new responsibilities and potential risk.

The government's guidance to organisations on the offence of failure to prevent fraud (Guidance) is intended to assist organisations to develop and implement appropriate procedures and policies to combat fraud occurring in their businesses. Its publication paves the way for the new failure to prevent fraud (FTPF) offence, introduced by the Economic Crime and Corporate Transparency Act 2023 (ECCTA), to come into effect in just over nine months' time; by 1 September 2025, all in-scope organisations will need to have in place reasonable procedures to prevent fraud being committed by their associated persons (such as employees, agents, subsidiaries and other persons that perform services for or on their behalf) so that they have the best chance of raising a defence if prosecuted for failing to prevent such wrongdoing.[1]

A brief overview of the FTPF offence

Under the FTPF offence, a "relevant organisation" anywhere in the world will be criminally liable where a person associated with it commits a UK fraud intending to benefit, directly or indirectly, the organisation (or any person to whom the associate provides services on behalf of the organisation, such as a client) and the organisation did not have reasonable procedures in place to prevent the fraud. The FTPF offence is effectively one of strict liability for the organisation as prosecutors will not need to show that the organisation's leaders authorised or had knowledge of the fraud. However, an organisation will not be guilty if it was itself a victim or intended victim of the fraud.

[1] For a more detailed review of the offence and its elements, see our previous publications: Revealed at last: The government publishes its proposals for a new failure to prevent fraud offence and The Economic Crime and Corporate Transparency Act receives Royal Assent – now the hard work begins

The offence will apply to “large organisations” operating in any sector (including commercial businesses, charities, NGOs and public bodies) which, in the financial year preceding the year of the fraud offence, satisfied at least two of the following requirements: turnover of more than £36 million; total assets of more than £18 million; and an average of more than 250 employees.

A schedule to the ECCTA lists the in-scope fraud offences. These currently comprise a set of core common law and statutory fraud offences (such as fraud, false accounting, fraudulent trading and cheating the public revenue) but the Secretary of State may amend the list at any time. Interestingly, the Guidance contains some useful hypothetical examples of how the offence will operate. It is notable that several of these are greenwashing and environmental scenarios, which may indicate where the authorities will be looking to focus their efforts.

Aims of the FTPF offence

The ECCTA is part of the package of measures introduced by the previous government to address the escalation in economic crime in the UK. Fraud is particularly prevalent and accounts for over 40% of all crime nationally.[2] The FTPF offence makes it easier to hold organisations criminally liable for fraud committed by those working for or with them and should enable the successful prosecution of businesses which fail to prevent such wrongdoing.

A second, but just as important, aim of the ECCTA is to drive change in corporate culture. In this respect the FTPF offence is intended to replicate the success of a similar offence introduced under the Bribery Act 2010, which is widely credited with promoting the introduction of corporate anti-bribery measures and the creation of a commercial business culture in which corruption is not acceptable.

Key principles in the Guidance

The Guidance is built around six key principles, which are intended to be “flexible and outcome-focussed”, and provides comment and recommendations on specific issues. However, although it confirms that a departure from the suggested procedures will not automatically mean an organisation does not have reasonable fraud prevention procedures in place, even strict compliance with the Guidance will not necessarily in itself amount to having reasonable procedures, for example where a business faces unique risks that it has not addressed. Ultimately it will be for a court to decide whether, in the circumstances and on the balance of probabilities, procedures adopted by a business were reasonable.

Top level commitment

Fostering an open culture for reporting fraud concerns is central to the Guidance and is identified as a key responsibility for senior management. Senior management is urged to set the tone for ethical behaviour and clearly communicate the organisation’s zero-tolerance stance on fraud. This commitment needs to go beyond verbal statements; senior management is

[2] According to National Crime Agency figures: Fraud - National Crime Agency

expected to demonstrate accountability by actively engaging in anti-fraud measures and supporting training and resources for fraud prevention.

Whilst most organisations will be familiar with the need for top level commitment (this principle is also set out in the existing guidance for other failure to prevent offences), creating an anti-fraud culture may require further introspection. If effective cultural shift is to happen, incentives and justifications for why associated persons might engage in fraudulent activities will need to be identified before they can be addressed.

Risk assessment

The Guidance helpfully acknowledges that it is not possible to anticipate all potential fraud risks and suggests that organisations adopt the "fraud triangle" as a framework for developing fraud risk typologies. The fraud triangle consists of three elements: opportunity, motivation and rationalisation and stems from Donald Cressey's (1953) book, Other People's Money: A study in the Social Psychology of Embezzlement. It's typically used by audit professionals and standard setters to identify and explain fraud. The emphasis on "motivation" and "rationalisation" – why people commit fraud and how they justify it - suggests that organisations fostering the right culture, as discussed above, including by expressly challenging certain mindsets, will be a key part of evidencing the existence of reasonable (and effective) procedures.

The Guidance also suggests that the anti-fraud measures contained in future prosecutions and deferred prosecution agreements (DPAs) may be useful for other businesses in the same sector. This seems wishful thinking given that 13 years of failure to prevent bribery haven't yielded much, if any, guidance on adequate procedures. That said, as examples emerge of fraudulent conduct – either through prosecutions and DPAs or through organisations' own internal investigations – these will no doubt be a useful data source for refining risk assessments.

Proportionate risk-based prevention procedures

As expected, the Guidance provides that any fraud prevention procedures should be proportionate to the fraud risks identified. Most importantly the Guidance acknowledges the varying degree of control an organisation may have over its associated persons; for example, a company will have greater control over the conduct of an employee than a third-party contractor. Accordingly, there may be instances where it is not possible to implement mitigation for an identified risk. In such circumstances, the Guidance suggests that the name and position of the person authorising the decision not to implement a procedure should be documented – emphasising the emerging theme of increasing accountability for individuals with responsibility for financial crime compliance.

Given that the offence applies to organisations across a broad range of sectors, the Guidance helpfully clarifies that it is not necessary or desirable for organisations to duplicate existing work done to comply with other regulations on financial reporting, environmental, health and safety or competition matters (for example). What's key is that organisations are satisfied that the procedures they have in place are sufficient to prevent the

fraud risks identified. As such, compliance processes under other regulations will not automatically qualify as “reasonable procedures” for the purposes of providing a defence but they may be a starting point.

As we have seen with other failure to prevent offences, implementing prevention procedures under the Guidance is far from a “tick the box” exercise.

Due diligence

This is one area where perhaps the Guidance lacks substance, stating simply that organisations should take a “proportionate and risk-based approach”. In practice, many in-scope organisations will already have in place sophisticated due diligence processes dealing with aspects such as the onboarding of agents and other third parties and in the context of mergers or acquisitions. The Guidance notes that these may not be an adequate response to tackle the risk of fraud but only sets out a handful of best practice suggestions, including the use of “third party” tools and “consultants” with no further detail as to who or what these should be.

Given the importance of third party due diligence in any financial crime compliance programme, it is perhaps surprising that the government has not offered more guidance in this regard.

Communication

The organisation must ensure that its policy against fraud is clearly communicated to everyone in the business. The Guidance stresses that training is key and should be commensurate with the risk faced by individual representatives or functions. This section also notes that an effective whistleblowing process is one of the best ways to detect fraud. The Guidance suggests that where one is already in place, it should be reassessed for suitability for the new FTPF offence and refers to government-produced guidance for employers in this area. A whistleblowing policy is increasingly being considered a “must have” for large organisations, even where one is not required by a sector regulator.

Monitoring and review

Organisations will be expected to monitor their fraud detection and prevention procedures and review them in the light of events and as risks change. This area of the Guidance is another example of the potential increased burden on businesses emanating from the FTPF offence. In-scope organisations will be expected to monitor how effective their policies are in detecting attempted fraud beyond that of which they are themselves the victim - something which may require an extension of existing policies. They will have to consider their approach to investigating suspected fraud, including identifying the triggers for an investigation, how one would be conducted, the potential need for external investigators and so on. They will also be expected to monitor the effectiveness of their fraud prevention measures through internal (and potentially external) reviews and make adjustments where needed. These requirements are likely to be new to many organisations and require considerable thought, analysis and documenting of findings and outcomes, all of which will take time and money.

Key Takeaways

Nine months may sound like plenty of time to prepare but the thorough analysis of risks faced, review of existing policies and planning for potentially fraudulent situations required will entail careful and detailed consideration by in-scope organisations. To get a head start, in-scope businesses should consider:

- reviewing and updating their own particular fraud risk typologies, identifying areas of potential criminality and vulnerability;
- reviewing the scope and ambit of any existing anti-fraud policies and whether they will need extending or amending;
- seeking advice on industry standards, bearing in mind that these are not government-approved or definitive;
- reviewing in-house communications and training, with a clear tone being set from the top and echoed throughout all levels of staff;
- establishing, where needed, policies and procedures for dealing with attempted or suspected fraud, and maintaining records of how such events are dealt with;
- reviewing any whistleblowing procedures already in place, or instituting such a policy if none exists;
- seeking legal advice on the scope of the FTPF offence particularly in group company situations, where subsidiaries are involved or where the business operates overseas. The Guidance makes it clear that these are technical legal matters on which it cannot advise.

The Home Office landing page which contains links to all ECCTA-related documents is here: Offence of 'failure to prevent fraud' introduced by ECCTA - GOV.UK.

Contacts

Satindar Dogra
Partner
Tel: (+44) 20 7456 4316
Mob: (+44) 7795601684
satindar.dogra@linklaters.com

Alison Saunders
Consultant
Tel: (+44) 20 7456 3812
Mob: (+44) 7876651873
alison.saunders@linklaters.com

Gavin Lewis
Partner
Tel: (+44) 20 7456 4209
Mob: (+44) 7585960504
gavin.lewis@linklaters.com

Elly Proudlock
Partner
Tel: (+44) 20 7456 2594
Mob: (+44) 7785428268
elly.proudlock@linklaters.com

For general enquiries please contact

Linklaters LLP
One Silk Street
London EC2Y 8HQ

Tel: +44 20 7456 2000
Fax: +44 20 7456 2222

www.linklaters.com