



## Peters & Peters

---

27 November 2024

Earlier this month, the government released [guidance](#) on the new corporate criminal offence of failure to prevent (FTP) fraud. In the first of a series of four articles, we analysed what [companies and their advisers need to know about this significant development](#). In this second instalment, we explain how ESG fraud is likely to be a key vector of enforcement under the new offence.

The government's guidance features eight hypothetical examples designed to explain the scope of the FTP fraud offence. Strikingly, three of the eight examples feature an ESG-related fraud. This is no mistake. It marks a clear indication from government regulators that ESG fraud is an enforcement priority. It is important for companies to understand that the way their businesses intersect with ESG issues can lead to corporate criminal liability; we have used a case study, below, to explain.

### **Hypothetical case study**

An investment fund provider, Company A, promotes a range of ESG-integrated investment products. As part of Company A's promotional materials, it makes statements about the policies, procedures and proprietary tools applied to operate its ESG products. While Company A did have policies and procedures in place to uphold the integrity of its ESG products, these were not consistently followed in practice. Additionally, Company A's proprietary tools did not effectively filter investments as advertised; resulting in investments being made in companies from industries that were intended to be excluded from its ESG products. It is unclear to what extent these deficiencies were known by the senior management of Company A. However, some of Company A's employed investment professionals had knowledge that its promotional materials for the ESG products were misleading, but allowed investors to rely on these materials to make investments in the ESG products regardless.

### **Has Company A committed the FTP fraud offence?**

The FTP fraud offence, which applies to "large organisations"<sup>1</sup> and their subsidiaries and enters into force on 1 September 2025, is committed if someone associated with the company, such as an employee, agent or person providing services on its behalf, commits fraud with the intention of benefiting the company or its clients. The company has a complete defence if it can demonstrate that it had "reasonable" fraud prevention procedures in place.

In the case study, the investment professionals commit a base offence of fraud by false representation. They dishonestly make a representation to potential investors by using promotional materials they know to be untrue or misleading and do so with the intention of soliciting investment. The investment professionals are associated with Company A as they are employees. The base fraud was also

committed with the intention of benefitting Company A as its purpose was to secure investment for Company A's ESG products.

As a result, Company A will be criminally liable for failure to prevent fraud unless it can demonstrate that it had "reasonable" fraud prevention procedures in place. While Company A had policies and procedures to ensure representations it made in relation to its ESG products were accurate, these were not consistently followed. Subsequent investigation reveals the reason these policies were not followed is that Company A had not set up controls to monitor the implementation and effect of its policies and procedures. Consequently, Company A was unable to spot deficiencies such as poor communication of the procedures and a lack of commitment from senior management.

Unable to demonstrate that it had reasonable procedures in place, Company A would be criminally liable under the new offence and subject to an unlimited fine.

### **Exploring liability**

The government's guidance explains that each company will possess a unique combination of opportunities, motivations and rationalisations for committing fraud.<sup>2</sup> To have a "reasonable" fraud prevention procedure involves addressing these three "typologies". Therefore, where a company makes regular representations about its ESG products (opportunity) in which its employees receive commission for securing investments (motivation) and the company's culture is quietly tolerant of fraud (rationalisation) there is a heightened risk of fraud for which proportionately stronger fraud prevention procedures must be implemented to avoid criminal liability.

It is also notable that in the hypothetical case study, Company A could not have avoided liability by subcontracting the administration of its ESG products to a third party. Not only can Company A be liable for the fraudulent acts of employees, but also those agents or persons who provide services on its behalf.

### **The enforcement outlook**

The FTP fraud offence will be most effective when used by prosecutors as an add-on charge in a matter involving wider criminality. This is because the offence lowers the threshold of corporate criminal liability, making it easier for prosecutors to secure convictions and persuade companies to enter deferred prosecution agreements.

Accordingly, broader regulatory trends in ESG fraud are important. At the end of May this year, the Financial Conduct Authority (FCA) introduced its anti-greenwashing rule (AGR). The FCA already has rules on misleading statements, but the AGR was introduced to signal that greenwashing is a priority to the regulator and provide it with an explicit rule to challenge non-compliant firms. The Competition and Markets Authority and Advertising Standards Agency introduced similar rules on greenwashing in 2021 and 2023 respectively.

These bespoke regulatory regimes have the ability to target and uncover the type of fraudulent conduct which could result in criminal enforcement of the FTP fraud offence. For example, via a joint FCA and SFO prosecution.

In a regulatory environment where priorities are shifting to ESG and the number of tools for tackling fraud are increasing, it is inevitable that Company A will not be alone in facing the sharp end of the ESG enforcement stick.

## **Other resources**

Peters & Peters will continue to analyse ESG enforcement trends and has created an [ESG enforcement tracker](#) for this purpose.

The next instalment in this series will consider the extra-territorial impact of the new FTP fraud offence guidance.

## **Footnote**

<sup>1</sup> 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.

<sup>2</sup> See reference to opportunity, motivation and rationalisation in chapter 3.2 of the guidance.