HERBERT SMITH FREEHILLS

Corporate Crime Briefing

Failure to prevent fraud – what are the implications of the new offence?

31 MAY 2023
London

Table of contents

Related links

Herbert Smith Freehills

FSR and Corporate Crime Notes blog

1. Introduction

The new failure to prevent fraud offence was introduced into the Economic Crime and Corporate Transparency Bill (the "Bill") during its progress through the House of Lords. Following our initial briefing regarding the proposed offence, we analyse the latest developments, key elements of the new offence (as currently drafted), areas of ongoing debate, and some practical illustrations of the implications of the new offence for companies who are planning the steps they may need to take in response to the new offence.

2. Parliamentary background and timing

The proposed new failure to prevent fraud offence follows a long-running debate regarding potential corporate criminal liability reforms, including, most notably, the Law Commission's options paper. The identified options included, among others, the introduction of a new failure to prevent fraud offence, and were discussed in our previous briefing. There are however certain differences between the Law Commission's recommendations and the Government's proposal, which are analysed further below.

The Bill did not initially contain a failure to prevent fraud offence, but the Government committed to add this following cross-party attempts to introduce a very broad-ranging offence during the Bill's initial progress through the House of Commons. The Government first proposed a failure to prevent fraud offence in amendments to the Bill on 11 April 2023, with further amendments proposed on 4 May 2023 by Lord Sharpe (Parliamentary Under-Secretary of State in the Home Office). A series of further draft amendments by Peers have also been debated, and on the whole rejected, and the Bill has now concluded in committee stage within the House of Lords. It will now move to the report

stage before it returns to the House of Commons for consideration. This briefing considers the most recent version of the Bill as it has emerged from Committee, but it therefore remains subject to further amendment.

The Bill is expected to receive Royal Assent before Parliament rises for the Summer recess, on 20 July 2023. It is less clear when the offence will be brought into force. The Government's Economic Crime Plan 2 (the "Plan") suggests it will be "introduced" in Q3 2023, but this seems ambitious given the need for guidance to be drawn up (and, hopefully, publicly consulted upon) and for companies to prepare. We expect that Q4 2023 or, more likely, H1 2024, would be a more realistic timeframe.

Further information about the introduction of the offence can be found in the Government-issued press release, impact assessment (the "Impact Assessment") and factsheet (the "Factsheet").

More information about the Bill generally can be found in our previous briefing. More broadly, introducing a failure to prevent fraud offence is part of the Government's wider legislative reforms and its strategy aimed at tackling high levels of fraud and enhancing enforcement, as detailed in its Fraud Strategy (May 2023) and the Plan. Further reforms to the identification doctrine are also expected in due course (as referred to in paragraph 6.16 and Action 39 of the Plan), although they do not form part of the Bill.

3. Failure to prevent fraud: an overview

Our previous briefing summarised the key elements of the proposals.

As a reminder, a corporate offence (an "FTP Offence") is committed where:

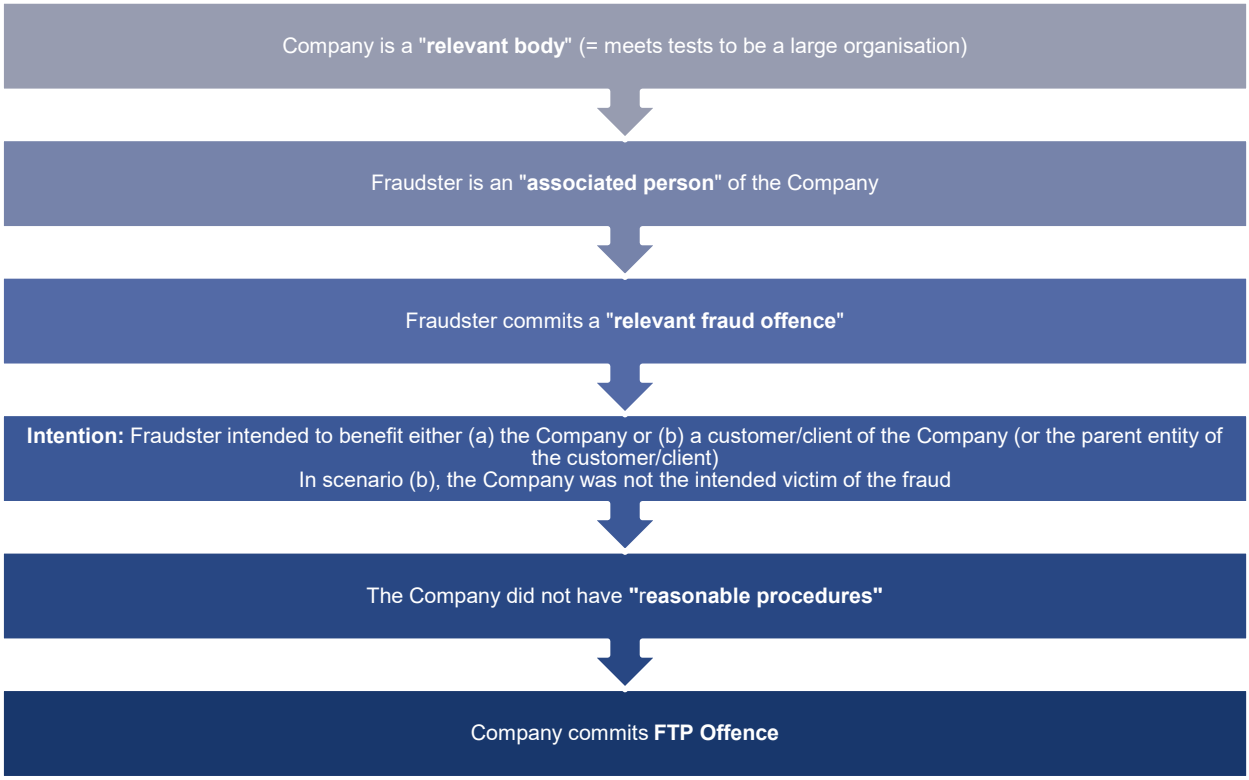
- an "associated person" of a "relevant body" commits a "relevant fraud offence" (all of these concepts are discussed further below);
- intending to benefit (directly or indirectly) the relevant body or any person to whom, or to whose subsidiary, the associate provides services on behalf of the relevant body; and
- the relevant body did not have in place reasonable fraud prevention procedures.

A relevant body can be a company or a partnership (and references in this briefing to a "company" or "corporate" are for convenience). However, the FTP Offence currently applies to large organisations only, defined (using the standard Companies Act 2006 definition) as organisations meeting two out of three of the following criteria: (1) more than 250 employees (2) more than £36 million turnover and (3) more than £18 million in total assets.

No FTP Offence is committed where the fraudster intended to benefit the client/customer of the relevant body, and the relevant body was itself a victim of the fraud offence (or was intended to be).

If convicted, an organisation may be liable to an unlimited fine.

Further practical examples are provided in section 5 below, and the components of the offence can be illustrated as follows:



4. In depth analysis of the new offence

We have set out below some more detailed analysis of the key elements of the FTP Offence and issues still to be clarified by the Government and legislative process.

Predicate offences

In England and Wales, a relevant fraud offence comprises:

- Fraud Act offences, comprising:
  - fraud by false representation,
  - fraud by failing to disclose information,
  - fraud by abuse of position,
  - obtaining services dishonestly, and
  - participation in a fraudulent business;
- False accounting (section 17 of the Theft Act 1968);
- False statements by company directors (section 19 of the Theft Act 1968);
- Fraudulent trading (section 993 of the Companies Act 2006); and
- Cheating the public revenue.

(In Northern Ireland, the offences under the Theft Act 1968 are replaced by their equivalents under the Theft Act (Northern Ireland) 1969 and in Scotland the FTP Offence also applies to the common law offences of fraud, uttering and embezzlement.)

As can be seen from the above, the list of predicate offences that, if committed by an associate, can trigger the FTP Offence, currently only includes fraud and false accounting offences. A number of proposed amendments to the Bill during its progress through the House of Lords sought to expand the list to include money laundering as well as sanctions evasion offences, however these amendments have not been incorporated in the latest version of the Bill. It is possible that further offences will be added as the Bill continues to progress through Parliament, although the Government has not announced any plans to do so.

In any event, as the Bill is currently drafted, the Secretary of State would have the power to pass secondary legislation to remove or add further predicate offences within scope of the FTP Offence, provided the offence is: (i) one of dishonesty, (ii) otherwise of similar character to those listed above, or (iii) a substantive money laundering offence (i.e. an offence under sections 327-329 of the Proceeds of Crime Act 2002). The Government has stated in the Factsheet that any new offences added would be limited to economic crime and it has not indicated that it would seek to expand the current list. In this regard, we note in particular that a failure to prevent money laundering offence would be duplicative and overlap with existing anti-money laundering requirements under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (the "MLRs")[i].

The fact that further offences can be added by way of secondary legislation, without Parliamentary scrutiny, is of concern given the seriousness of the FTP Offence and the potentially broad/uncertain ambit of offences "of a similar character" to fraud. We would suggest that any expansion of the FTP Offence should be subject to appropriate scrutiny and detailed consultation, and anticipate that this is an area on which interested parties may wish to consider lobbying or raising concerns via industry bodies before the Bill receives Royal Assent.

Finally, although the fraud offences within scope are currently limited in the way described above, we note that they can cover an extremely broad range of conduct. We expect it to be much more challenging in the context of the FTP Offence, as compared to the "corporate offence" contained in the Bribery Act 2010 (the "UKBA"), to assess how and why an associated person might commit an offence of "fraud". This will make the guidance (discussed below), and companies' risk assessments, of particular importance to the implementation of "reasonable procedures".

Associated person

Under the current proposal, an associated person is:

(a) an employee, agent or subsidiary; or

(b) someone otherwise performing services for or on behalf of the company

In relation to the second limb, clause 188(7) of the Bill provides that whether or not a particular person performs services for or on behalf of a relevant body is to be determined by reference to *all the relevant circumstances* and not merely by reference to the nature of the relationship between that person and the body.

The definition is similar to the one under section 8 of the UKBA. However, important differences arise in respect of the first limb of the test in the Bill. Under the UKBA, a subsidiary or agent *may* be an associated person, on examination of all the relevant circumstances (and an employee is rebuttably presumed to be an associated person). In contrast, for the purposes of the FTP Offence, a subsidiary, employee, or agent is automatically included within scope.

The current definition will capture a wide range of persons and activities, posing particular practical challenges in the context of subsidiaries, since it could capture instances where a subsidiary operates independently, and where such subsidiaries are not in fact performing services on behalf of their parent company. However, for the offence to be committed in this scenario, an intention on the part of the subsidiary to benefit the parent company (or its customer/client/parent) would need to be established.

One critical issue will therefore be whether, where a subsidiary commits a fraud which is directly for its own benefit, this will be taken as an intention to benefit the parent. The contrary view is taken in the Ministry of Justice statutory "adequate procedures" guidance for the purposes of the UKBA. This helpfully explains that "*the fact that an organisation benefits indirectly from a bribe is very unlikely, in itself, to amount to proof of*

the specific intention required by the offence. Without proof of the required intention, liability will not accrue through simple corporate ownership or investment, or through the payment of dividends or provision of loans by a subsidiary to its parent…". If the same interpretation of the FTP Offence is adopted (and there appears to be no reason why it would be different), this will help circumscribe the otherwise extremely significant impacts of making the parent entity liable for all frauds committed by a subsidiary.

Whilst the intention test provides some boundaries on the coverage of subsidiaries, our view is that it would be preferable for the FTP Offence to track more closely the UKBA offence and the failure to prevent the facilitation of tax evasion offences by providing that a subsidiary *may* – not *will* – be an associated person. The current drafting approach will add additional complexity to the scope of the offence and reasonable procedures, and appears to have been introduced without any clear rationale.

Aligning the scope of "associated person" to the UKBA approach would also be more closely aligned to the Law Commission's proposals which, although they did not exhaustively discuss how "associated persons" should be defined, noted that the definition might include employees and agents.

Relevant body

As mentioned, the FTP Offence only applies to large organisations. This is in contrast to other failure to prevent offences, which do not contain such a criterion and apply to all entities within the jurisdictional scope of the offence.

The Government has not provided any rationale for why small and medium businesses ("SMEs") should be exempt from the new offence, although it has noted in the Impact Assessment that "*the exclusion of small and medium-business will reduce the possible benefits and the potential for cultural change. However, it is possible that small and medium-businesses may adopt some of these practices resulting in spill-over benefits*."

The scope of the offence has been subject to recent debate in the Lords, with some commenting that fraud committed by SMEs can be as damaging as the conduct of larger organisations, and that SMEs should also be encouraged to enhance their fraud prevention procedures. Certain Lords have stated that the size of the organisation could be taken into consideration at the public interest stage of the Full Code Test for Crown Prosecutors (i.e. in determining whether a prosecution should be brought in a particular case), rather than SMEs being excluded from the offence altogether. There is also a view that large organisations are most likely to have counter-fraud procedures, and it is odd to introduce an offence targeting the business segment for which it is least relevant.

A counter-argument is that the FTP Offence will be burdensome to business[ii], and that, particularly in the current economic climate, it is not appropriate to require SMEs to adopt additional compliance procedures of uncertain merit (the Government's Impact Assessment states that it is unable to quantify the benefits of the FTP Offence, and the non-monetary benefits are vaguely and aspirationally summarised as follows: "*the [FTP Offence] may reduce fraud by increasing consumer confidence and ensuring more money is directed towards legitimate businesses. There is also a wider socio-economic benefit as a reduction in fraud could result in lower emotional harms, victim support costs and law enforcement and CJS costs*"). There has also been concern in the UKBA context that there is insufficient guidance tailored to SMEs, to support them in understanding what "adequate procedures" to adopt[iii]. These concerns will be exacerbated in relation to the FTP Offence, which is of more uncertain ambit.

We understand that this is an area which remains subject to active lobbying, and it is not certain whether the current SME exemption will survive. SMEs should be aware that, in any event, under the Bill's current provisions, the Secretary of State can amend the meaning of "large organisation" via secondary legislation, potentially bringing them into scope without further legislative scrutiny.

Jurisdictional scope

Under clause 188(11) of the Bill, the FTP Offence applies to a body corporate or partnership wherever incorporated or formed. The Bill is otherwise silent on the jurisdictional scope of the new FTP Offence.

Therefore, it appears that the jurisdictional scope of the offence will depend on the jurisdictional scope of the underlying (predicate) offence committed by the associate. In very general terms, in terms of jurisdiction in

England and Wales, for most of the in-scope fraud offences the requirement is that a 'relevant event' occurred in England or Wales. For offences under sections 1 to 4 of the Fraud Act (fraud by false representation, fraud by failing disclose information and fraud by abuse of position), it will be enough that the intended gain or loss occurred in England or Wales.

According to the Impact Assessment, foreign domiciled corporates would only be impacted to the extent that they operate a UK branch or operate a UK subsidiary. However, the Factsheet states that: "*If an employee commits fraud under UK law, or targeting UK victims, their employer could be prosecuted, even if the organisation (and employee) are based overseas*" which would suggest a potentially much broader scope. Based on the current draft legislation, we believe the Factsheet is correct and the Impact Assessment is wrong. In other words, a non-UK company could in theory commit the FTP Offence, irrespective of whether it has a UK branch or subsidiary, if its associated person commits an offence of fraud within UK jurisdictional scope. In practice, there could of course be considerable practical challenges in investigating or prosecuting a non-UK company, depending on where it is based.

The Law Commission's position on this issue is that FTP offences should not generally operate extraterritorially by default unless there is a demonstrable need for extraterritoriality.

It remains to be seen whether any further amendments are introduced to define (or indeed limit or expand) the jurisdictional scope of the FTP Offence. We strongly concur with the Law Commission's recommendation, and note that, when combined with the broad scope of "associates", there is scope for a significant compliance burden if the FTP Offence is extended to UK parent companies in relation to the conduct by their loosely associated overseas subsidiaries, with no intended UK victims, and over which the UK parent has no formal control.

Reasonable procedures guidance

The Bill envisages that the Secretary of State will be required to publish guidance about procedures which relevant bodies can put in place to prevent associated persons from committing fraud offences (clause 192). As is the case with the other "failure to prevent" regimes already in place in the UK, this guidance on "reasonable procedures" will be of critical importance for companies seeking to understand, and minimise the risk of liability under, the FTP Offence. The Impact Assessment states that the requirement for "reasonable procedures" will place a lesser burden on organisations than requiring "adequate procedures", as under the UKBA.

We expect that the guidance is likely to be relatively high level and principles-based, given the very broad range of conduct which could fall within the scope of the FTP Offence. It is not clear if there will be a public consultation on the guidance[iv], although we hope that this will be the case – both the UKBA guidance and the guidance for the purposes of the "failure to prevent the facilitation of tax evasion" offences under the Criminal Finances Act 2017 (the "CFA") were consulted upon, and relevant changes were made as a result.

More generally, given the likely necessarily high-level nature of the statutory guidance to be issued in due course on the FTP Offence, we consider that this is another area in which the Government should follow the approach taken under the CFA and provide for the Secretary of State to approve industry guidance on reasonable procedures (see, for example, the UK Finance guidance for the financial sector). The provision of formal guidance which is appropriately sector-specific and tailored to the types of frauds which are most likely to arise in a given sector will support organisations in ensuring that they have appropriate controls in place. Industry bodies will also be best placed to assess the types of controls that are already in place within the sector and will be relevant in this context or can readily be repurposed, minimising the burden on companies who might otherwise consider that they need to implement an entirely new anti-fraud programme from scratch.

Finally, the Government has not yet indicated when it might be reasonable for a large organisation not to have procedures in place and it will be important for the guidance to be issued in respect of the FTP Offence to deal with this point. The guidance provided in relation to the CFA offences notes that, where a relevant body has fully assessed all the risks and they are considered to be extremely low and the costs of implementing any prevention procedures are disproportionate or cost-prohibitive in relation to the negligible risks faced, it may be reasonable not to expect that body to have prevention measures in place.

5. Practical implications – how would some common frauds be treated by the Bill?

Based on the current drafting of the Bill, the following scenarios are likely to involve the commission of an FTP Offence (subject to the availability of the reasonable procedures defence, and assuming that the company in question falls within the definition of a "large organisation"):

A junior employee of a regulated entity dishonestly mis-sells a financial product by mispresenting its suitability to customers, seeking to make increased sales for the company (and thereby earn a larger bonus or commission).

The individual will automatically be considered an associated person and could have committed a relevant fraud offence. Although their primary intention will have been to benefit themselves (rather than their employer), it seems unlikely that the company would be able to avoid committing an FTP Offence in circumstances where it would have been clear to the employee that the company would also benefit from the increased sales.

This is one scenario in which the FTP Offence will increase scope for corporate liability in that misconduct by a junior employee can result in corporate criminal liability.

A mid-level accountant fraudulently inflates a company's earnings by (dishonestly) instructing staff to recognise income in the wrong accounting period, or understate the company's losses.

Both the accountant and individual employees involved are associated persons, and could have committed a false accounting offence. Whether this was intended to benefit the company would be a fact-specific determination but, if this could be established, the company could be criminally liable. As above, we expect this to be the case even if there is also a personal benefit to the CFO/individual employees in the form of bonuses etc.

By contrast, the FTP Offence is unlikely to apply in the following scenarios:

In a scenario where an employee commits expenses fraud or otherwise misappropriates company funds, the company will generally be the intended victim of the offence and no FTP Offence will be committed.

If an individual posts fraudulent adverts online or on social media platforms, they will not be considered an "associated person" of the hosting company (because they are a customer/user, not an employee, agent, subsidiary or service provider). Therefore, the platform would not be liable for an FTP Offence. The Government is however proposing to introduce a new legal duty via the Online Safety Bill requiring social medial platforms and search engines to prevent paid-for fraudulent adverts appearing on their services.

An individual fraudster obtains funds from a bank's customer via an authorised push payment scheme. They are paid into another account at the same bank and then immediately transferred overseas.

The fraudster is not providing any service to the bank that could render it an associate and so (absent complicity by a bank employee) the bank would not fall within scope of the FTP Offence for this type of conduct.

There are therefore significant fraud typologies which will not be addressed by the introduction of the FTP Offence. There is said to be an "epidemic of fraud" being experienced in the UK, and the press release accompanying the introduction of the offence noted that fraud now comprises 41% of all criminal activity. We would suggest that this offence will be expensive for companies but will do little to address the frauds and scams that are so damaging to individuals and companies alike. It will be critical, therefore, that the Government continues to progress steps that may actually reduce the incidence of fraud, including some of the measures set out in the Economic Crime Plan 2 and, more broadly, ensuring appropriate funding for law enforcement and the criminal justice system.

6. Commentary

There are a number of key issues still to be determined in the latest version of the Bill, not least the jurisdictional scope of the offence. The fact that the Government can also expand the scope by including further offences and altering the definition of a "relevant body" by way of secondary legislation also presents concerns. Companies should therefore continue to monitor the progress of the Bill through Parliament to understand how the FTP Offence will apply in its final form.

Impacted organisations will in due course need to assess the risks of fraud within their business, including in relation to overseas subsidiaries, and, once further guidance is published, ensure they have in place, to the extent they do not have already, adequate anti-fraud procedures. We anticipate that for many organisations this will include mapping and documenting existing anti-fraud procedures and why they are considered to be responsive to the identified fraud risks.

We would suggest that steps that companies could be considering now include: socialising the incoming offence within the organisation; considering who the owners and stakeholders for any FTP Offence implementation project will be; considering the approach to group wide as opposed to UK compliance; considering when the project will be commenced; and how it will be resourced. Companies and trade organisations may also wish to consider continuing to make representations on some of the issues raised in this briefing or other points of concern, as the Bill finishes its progress through Parliament.

For more information on the FTP Offence, contact one of the authors of this briefing or your usual HSF contact.

7. Contacts

Susannah Cogman, Partner
T +44 20 7466 2580
susannah.cogman@hsf.com

Brian Spiro, Partner
T +44 20 7466 2381
brian.spiro@hsf.com

Robert Hunt, Partner
T +44 20 7466 3423
robert.hunt@hsf.com

Kate Meakin, Partner
T +44 20 466 2169
kate.meakin@hsf.com

Elizabeth Head, Of Counsel
T +44 20 7466 6443
elizabeth.head@hsf.com

Eamon McCarthy-Keen, Associate
T +44 20 7466 3776
eamon.mccarthy-keen@hsf.com

Clara Browne, Associate
T +44 20 7466 3792
clara.browne@hsf.com

If you would like to receive more copies of this briefing, or would like to receive Herbert Smith Freehills briefings from other practice areas, or would like to be taken off the distribution lists for such briefings, please email subscribe@hsf.com.

[i] The MLRs impose obligations on the regulated sector to have in place appropriate policies and procedures, including in relation to the conduct due diligence and ongoing monitoring to mitigate the risk of money laundering and terrorist financing, with the possibility of criminal penalties for breach, rendering a separate corporate offence of failure to prevent money laundering unnecessary in our view.

[ii] Even focussing only on large organisation, the Impact Assessment suggests the introduction of the offence will involve set-up costs for business of £357.6 to £451.8 million, with a central estimate of £439.1 (2020 prices) in year 1, and estimated ongoing costs of £47.1 to £61.0 million, with a central estimate of £59.5 million (2020 prices) every year from years 2-10.

[iii] See for example the House of Lords Select Committee on the Bribery Act's Post-Legislative Scrutiny Report in 2019, which recommended, inter alia, that "the Ministry of Justice should, in consultation with representatives of the business community, and especially of SMEs, expand the section 9 Guidance to give more examples and to suggest procedures which, if adopted by SMEs, are likely to provide a good defence."

[iv] The Bill contains a requirement for the Secretary of State to consult with the Scottish Ministers and the Department of Justice in Northern Ireland.