Loss Prevention Standards – Financial Lines

Failure to Prevent Fraud

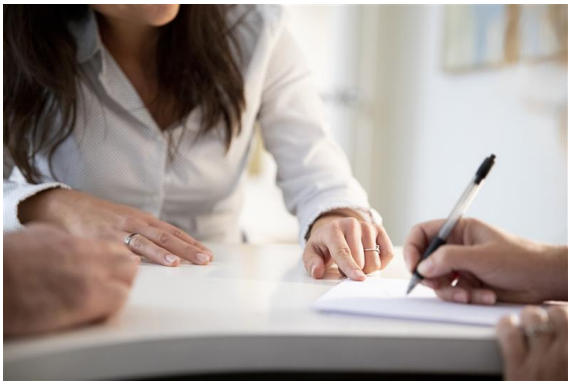
Version: 1.0
Date: 2nd December 2024

A guide on the statutory offence of failing to prevent fraud, preventative procedures to consider and a defence to prosecution.

AVIVA

Failure to Prevent Fraud

Introduction



According to UK government statistics, fraud is the *"most common offence in this country"*[i]. Between September 2021 and September 2022, 41% of all crime was fraud, despite fraud being generally underreported[ii].

The introduction of a new offence of Failure to Prevent Fraud within the Economic Crime and Corporate Transparency Act 2023 is designed to help tackle fraud.

Companies caught by the act could be subject to criminal liability, unlimited fines, reputational damage, and potential civil claims. The Failure to Prevent Fraud offence will come into force on 1 September 2025, so businesses should use this time to prepare for the upcoming changes.

D&O and Crime policyholders should also be aware that, in light of this new offence, they are likely to be required to provide more evidence of fraud prevention procedures to their insurers and should expect more Risk Management questions surrounding their fraud prevention governance.

This guide includes an overview of the new offence, and how businesses can protect themselves and their reputation.

What is "ECCTA"?

The **Economic Crime and Corporate Transparency Act 2023 ("ECCTA")** is a new piece of legislation that applies to specific UK businesses. As part of a raft of new measures[iii], ECCTA also creates a new offence, the Failure to Prevent Fraud.

The **"Failure to Prevent Fraud"** offence

The Failure to Prevent Fraud **("FTPF")** attributes criminal responsibility to companies for fraud offences. Specifically, it provides that:

"A relevant body which is a large organisation … is guilty of an offence if, in a financial year of the body … a person who is associated with the body ("the associate") commits a fraud offence intending to benefit (whether directly or indirectly) (a) the relevant body, or (b) any person to whom, or to whose subsidiary undertaking, the associate provides services on behalf of the relevant body".

What is the consequence of non-compliance?

Companies caught by ECCTA could be subject to criminal liability, unlimited fines, reputational damage, and potential civil claims.

All companies should therefore be giving careful consideration to whether or not ECCTA will apply to them, and if required, take immediate steps to protect themselves from the potential liabilities.

Does it apply to my business? What **is a "large organisation"?**

The FTPF offence applies to any corporate body or partnership (or a collective group of companies) who is a "large organisation". A "large organisation" is body (or group) which (in the financial year preceding the year of the fraud offence (see below) met two or all of the following criteria:

- A turnover of more than £36m;
- More than £18m on the balance sheet; and / or
- More than 250 employees.

If your company or group of companies meets two or more of these criteria, the FTPF offence potentially applies to you.

It may, however, be worth noting that the Home Office guidance published on 6 November 2024 relating to the FTPF offence (the "Guidance")[iv] states that *"although the offence … applies only to large organisations, the principles outlined in this guidance represent good practice and may be helpful for smaller organisations"*.

Who are "associates"?

Associates are defined by ECCTA Section 199(7) as employees, agents, and subsidiaries.

Importantly, associates also include those *"otherwise performing services for or on behalf of the body"*. This broad definition could include third parties such as experts or sub-contractors.

A different emphasis

It is likely that your business already has anti-fraud policies and procedures. However, those policies and procedures may have been produced in anticipation of the company or its clients being the *victims of* fraud and therefore had the primary intention of protecting the company and / or its clients from fraud committed *against* them. For example, an employee misappropriating client funds would render both the client who loses funds and the company which suffers reputational damage victims of the fraud.

The FTPF offence has the opposite emphasis – it will be committed if the company and / or its clients *benefits from* fraud. For example, an employee securing more work as a result of understating a client's financial performance to reduce its tax burden would benefit both the company (further fees) and the client (lower taxes).

It is, however, important to note that the FTPF offence is an addition to existing risks and offences, not a replacement. Existing policies and procedures remain important safeguards against existing fraud risks.

Is there a defence to failing to prevent fraud?

Under ECCTA Section 199(4), companies will have a defence to the FTPF offence if they can show one of the following:

1. *Prevention procedures that were "reasonable in all the circumstances"* (or)
2. That *"it was not reasonable in all the circumstances to expect the body to have any prevention procedures in place".*

Each of these are considered below.

What are "reasonable" prevention procedures?

All companies potentially affected should be carrying out a review of internal procedures. The Guidance contains six principles which it states should inform the prevention procedures. In our view, four key areas of focus may include:

1. Conducting a Risk Assessment
2. Reviewing and improving procedures
3. Considering the potential impact of third parties
4. Maintaining proper records

It should be noted that demonstrating an overall cultural shift towards fraud prevention should be considered at each stage.

1. Conducting a risk assessment – four key questions

The starting point for preparing for the FTPF offence coming into force will be carrying out a risk assessment. This should include consideration of the following:

- What is ***"reasonable in all the circumstances"***?

The extent to which your company puts in place prevention procedures must be *"reasonable in all the circumstances"*. The Guidance suggests companies start with classifying the types of associates providing services and considering the opportunity and motives each may have to attempt a fraud. Our view is that the following should also be considered:

  - The markets in which your company operates (both in terms of target market and jurisdictions);
  - The types of services / products your company provides;
  - The clients of your company;
  - The third parties with which your company interacts in the course of its business, including any distributors;
  - The size of your company and its corporate structure;
  - The financial resources of your company;
  - Your company's existing infrastructure; and
  - The existence or otherwise of relevant external / independent regulation and how that is relevant.

- Which fraud offences might we be exposed to and who might commit them?

The risk assessment should identify your exposures to ensure that the preventative procedures are "relevant" to them.

- What existing anti-fraud procedures and measures do we currently have in place?

If your company already has reasonable and robust anti-fraud procedures protecting it and its customers / clients from being victims of fraud, you are unlikely to have to reinvent the wheel. However, the introduction of the FTPF offence does present a good opportunity to review those procedures generally and, in particular, test their robustness against how (if at all) they prevent your company and its customers / clients being the potential beneficiaries of fraud as well as the potential victims.

- What is our corporate **"culture"** and what internal pressures exist?

This is perhaps where the emphasis shift within the FTPF offence is most relevant. Whilst objective-setting is of course a legitimate and normal part of company life, placing significant pressure or expectations on associates (for example, through bonus structures, promotion prospects, or setting high targets – whether they be related to financial targets, client wins, client retention or client satisfaction) may also foster an environment where associates are tempted to commit fraud offences which benefit the company or its clients. Highly pressurised companies may well need more robust procedures than companies where such pressures are not as great.

Importantly, the risk assessment should be recorded, retained and reviewed periodically. For example, it could be reviewed annually or when there are relevant developments in the business (such as a merger / acquisition, a change in work type or a change in client type).

2. Reviewing and improving procedures

Every company is different. What is *"reasonable in all the circumstances"* will be different between companies. However, we would expect all relevant bodies to consider the need for some or all of the following:

- Client onboarding / customer due diligence **("CDD")** / know your customer **("KYC")** - Client onboarding should allow for:
    - Properly identifying the client and checking whether it is subject to sanctions / restrictions;
    - Gathering additional information to understand the nature of the client's business and identify risk areas – potentially leading to enhanced due diligence if this process uncovers any issues; and
    - Ongoing monitoring.

- Recruitment practices – It would be sensible, in addition to the usual recruitment considerations, to consider gathering similar information to that required by KYC in relation to new recruits. It may be that search results reveal fraud 'red flags', such as previous behaviour or questionable connections or views. The practices should be commensurate to the risks associated with the role being recruited for.

- A specific anti-fraud policy – This should clearly set out both the company's attitude to fraud and, in light of the FTPF offence, its responsibilities in preventing it. It should summarise the systems and procedures in place, encourage reporting and set out the action that will be taken if associates commit fraud offences. This can be an effective counterbalance against some of the cultural pressures that can exist in companies discussed above. When produced, the policy should be accessible and well-communicated.

- Peer review / work review / audit procedures –Anyone considering committing a fraud offence is less likely to do so if they know that their work is routinely reviewed. A good peer review procedure will be carried out at regular and frequent intervals, on files or projects selected at random, will be independent, will cover all aspects of a file or project (including financial aspects) and will provide for any action points or training needs to be followed up. It should also be recorded. Associates with roles that allow them to work alone i.e. without routine oversight, should be prioritised.

- Banking and payment procedures – Some (but not all) of the fraud offences will involve money. Accordingly, robust banking procedures which can be monitored in real-time and analysed subsequently should be put in place. For example, making sure that payments must be verified / signed off by a second person, or unusual / unexpected / discrepant receipts or payments are flagged internally.

- Whistleblowing policy – A fraud offence is usually discovered by someone working closely with the perpetrator. Whilst whistleblowing is, to a large extent, protected by law, the introduction of the FTPF offence represents a good opportunity for companies to implement a clear, accessible, well-communicated whistleblowing management system if they do not have one already or, for those that do, to ensure it applies to and encapsulates the offences within the FTPF offence.

- Investigation and disciplinary procedures – Having clear procedures whereby any suspected or reported fraud offences are investigated and dealt with appropriately (whether by way of employment disciplinary procedures, further reporting to the relevant authorities or both) can be an effective deterrent. These procedures should be linked to how reports generated by the whistleblowing policy are handled, since whistleblowing reports being improperly handled can lead to demotivation, escalation, and even public scandal.

- Technology / analytics – your company should consider the appropriate use of technology and / or analytics tools to detect any trends or unusual practices that could be indicative of fraud. For example, identifying that a particular associate uses one third party more than any other and then investigating why, or unusual payments / receipts being flagged.

- Focus during tender / bid processes – The risk of fraud (and ways to minimise it during the project or retainer) should also be assessed at the tender or bid stage.

- Training – your associates should be provided with training on the FTPF offence and your company's anti-fraud procedures. That training should be recorded and repeated periodically (for example, annually).

LOSS PREVENTION STANDARDS

- Nominated teams / persons responsible – Having a particular team or person(s) responsible for procedures promotes accountability and helps to facilitate proper investigation and reporting.

- Agenda item at board / high-level meetings – Again, this will show that your company takes its responsibilities seriously and would provide a regular opportunity to review the success and adequacy of the procedures in place. The Guidance cites "top level commitment" as one of the six principles.

- Participation in cross-industry efforts – It may be possible to join forces with other companies within your industry to share insights and experiences which can be incorporated into your procedures.

- Remuneration – your company's bonus structure could include incentives or bonuses which emphasise anti-fraud practices or reward fraud prevention. Consideration could also be given to the company's remuneration structure. A company with associates that are remunerated fairly, in line with or above market norms, may find its associates are less likely to commit fraud.

- Operational tests – Your company could consider carrying out an operational test of the company's procedures on a regular basis, once they are in place and embedded.

- Co-operation – the Guidance states that a willingness to co-operate and make full disclosure in the scenario where a fraud offence has been committed will be taken into account in any decision as to whether it is appropriate to prosecute your company at all.

As above, any procedures and policies put in place should be recorded, retained, and reviewed periodically.

3. Third parties performing services

Your company could also be held liable for the FTPF offence if a third party whom you have engaged to either provide services to you or on your behalf commits a fraud offence.

We anticipate that the reasonable prevention procedures expectations on you will be lower in respect of third parties' actions, given the likely reduction in control. The expectations may be lower still if that third party is also a large organisation (since the third party could then itself be prosecuted for the FTPF offence). However, given the potential risk to you, it would be sensible if, when engaging a third party, you consider the following:

- Partner onboarding – which requires a third party to outline the prevention procedures it has in place for you to assess. You could then consider recording your assessment criteria.
- Partner screening – so that you can review whether the third party has previously been involved with fraud (or even previously prosecuted for a fraud-related offence).
- Engagement terms – it may be possible for you and the third party to include prevention procedures or guarantees into your contracts / agreements with that third party.

Your assessment should then refer back to the *"reasonable in all the circumstances"* test.

4. Keeping a record

Finally, but importantly, the statutory defence states that it is *"for the relevant body to prove"* that it had reasonable prevention procedures in place. Your company should therefore keep records of whatever steps it takes to comply with the requirements of ECCTA. We consider that this will need to include copies of:

- The risk assessment carried out;
- Your CDD / KYC procedures;
- Your recruitment policy;
- Your fraud policy;
- Peer review / audit procedures (and the audits themselves);
- Banking procedures;
- Your whistleblowing policy;
- Investigation and disciplinary procedures;
- Training records;
- Relevant board meeting minutes; and
- Your partner onboarding.

The big question - is it reasonable to have no prevention procedures in place?

Finally, we consider the second limb of the defence, which provides that a company may have a defence even without any prevention procedures in place.

We expect circumstances in which it is reasonable for a company have no fraud prevention procedures in place whatsoever will be extremely rare.

In any event, just as ECCTA requires a company to prove it had reasonable prevention procedures in place, companies without any prevention procedures in place will also have to prove that that was reasonable. At the very minimum, therefore, we would expect a company to have carried out a risk assessment and for that risk assessment to conclude that it would not be reasonable in the circumstances for the company to have any prevention procedures in place. Therefore, a prudent business will walk through the above steps in any event.

Checklist

A generic Failure to Prevent Fraud Checklist is presented in Appendix 1 which can be tailored to your own organisation.

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

Sources and Useful Links

- Economic Crime and Corporate Transparency Act 2023 (legislation.gov.uk)
- Economic Crime and Corporate Transparency Act: failure to prevent fraud offence - GOV.UK (www.gov.uk)
- Fraud - National Crime Agency
- Guidance to organisations on the offence of failure to prevent fraud

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Appendix 1 – Failure to Prevent Fraud Checklist

Location	
Date	
Completed by (name and signature)	

	Failure to Prevent Fraud	Y/N	Comments
1.	Does the FTPF offence apply to my company? I.e. did my company, in the financial year preceding the fraud offence, have any two of (a) turnover more than £36m (b) more than £18m on the balance sheet and / or (c) more than 250 employees? OR (if my company is a parent company) did all the companies in the corporate group meet two or all of those criteria in the aggregate? [If it does not, the FTPF offence does not apply to your company. However, your company is still unlikely to want to be associated with fraud and could therefore still consider the below and this guide by way of good practice]		
2.	Have we carried out a thorough risk assessment, considering what prevention procedures would be reasonable in all the circumstances to put in place - taking into account the fraud offences we are potentially exposed to, our existing anti-fraud procedures and our culture?		
3.	Having done so, have we diarised for the risk assessment to be reviewed both when changes relevant to it occur and periodically?		
4.	Is our risk assessment properly saved for review and production if necessary?		
5.	Is there a proper plan for implementing and embedding all the procedures identified as reasonable in the risk assessment, which includes timescales and identifies persons responsible?		
6.	Are our client onboarding procedures robust, allowing us to properly know our client and assess any fraud risks arising from accepting them as a client?		

LOSS PREVENTION STANDARDS

7.	Is our recruitment robust, allowing us to assess the fraud risk associated with recruiting a particular individual?		
8.	Do we have a fraud policy that is accessible and well-communicated?		
9.	Do our working practices involve duality and checking?		
10.	Are our projects and employees peer reviewed / audited regularly? Are those reviews recorded and discussed with the employee?		
11.	Are our banking procedures sufficient to make it unlikely that an associate could commit a fraud offence unnoticed? For example, would unusual / unexpected transactions be flagged? Do transactions have to be approved by another person?		
12.	Do we have a whistleblowing policy that is accessible, well-communicated and which ensures potential whistleblowers are listened to and kept updated (so far as it is possible to do so) and reports are properly investigated?		
13.	Do we have procedures which allow for the proper investigation of suspected or reported fraud? Are our disciplinary procedures fair but robust?		
14.	Would the use of appropriate technology or analytics tools strengthen our position in relation to fraud? Is this kept under review?		
15.	Do our tenders / bid processes actively guard against fraud – both during the process itself and in ensuring projects are carried out non-fraudulently?		
16.	Are all employees trained in relation to the FTPF offence? Is it part of the induction process? Is that training repeated periodically? Is training (who has completed it, what it involves) recorded?		
17.	Is fraud prevention prioritised at the top of your company and filtered down appropriately? For example, are there specific people / teams responsible for it? Is it discussed at board level? Is your company part of any cross-industry discussions?		
18.	Once in place, are your procedures tested?		
19.	Are your partner onboarding procedures sufficient to allow you to assess their prevention procedures and screen them appropriately?		
20.	If a fraud offence is committed / discovered, do our procedures include provision to co-operate with and make full disclosure to the prosecuting authority?		

[i] https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-act-2023-factsheets/economic-crime-and-corporate-transparency-act-failure-to-prevent-fraud-offence

[ii] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

[iii] including reforming Companies House, increasing enforcement powers in relation to crypto assets and amending the Civil Procedure Rules to help support transparency

[iv] https://assets.publishing.service.gov.uk/media/67331b8ff407dcf2b561350a/Failure_to_Prevent_Fraud_Guidance_-_English_Language_v1.3.pdf

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

2nd December 2024

Version 1

ARMSGI2232024

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.