

Getting Ready: The New ‘Failure To Prevent Fraud’ Offence

What does the UK government's new guidance on the offence for failing to prevent fraud say, and what can organisations do to ensure compliance?

By 1st September 2025, organisations within scope should have implemented **reasonable procedures** in line with the new **corporate criminal offence** of “failure to prevent fraud” (FTPF offence).ⁱ Our briefing summarises the UK government’s recently published [Guidance](#)ⁱⁱ on the offence, and what organisations need to know to get ready.

The [Economic Crime and Corporate Transparency Act 2023](#) (ECCTA)ⁱⁱⁱ created the FTPF offence and has **three main objectives**:^{iv}

- | | | |
|---|--|---|
| 1. To hold organisations to account more easily for fraud committed by employees or associated persons that may benefit the organisation or its clients. | 2. To encourage more organisations to implement and/or improve fraud prevention procedures. | 3. To promote a major shift in anti-fraud culture within organisations , to help reduce fraud. |
|---|--|---|

The Guidance focuses on a **risk-based** approach, **proportionate** policies and procedures, demonstrable **commitment** from senior leaders, undertaking risk assessments, training, and **ongoing** monitoring and review.

What Is the Failure To Prevent Fraud Offence?

Organisations may be **held criminally liable** where:

- an employee, agent, subsidiary, or other “**associated person**” (including SMEs) providing **services** for/on behalf of the organisation;
- commits a fraud **intending to benefit** the organisation or their clients; and
- the organisation **did not** have reasonable fraud prevention procedures in place.

When Does The Offence Come Into Force?

Contact us today to find out more
info@fraud-sentinel.com

fraud-sentinel.com



- **1st September 2025.**
- Organisations will be expected to have implemented reasonable fraud prevention procedures **by this date.**
- The FTPF Guidance to organisations was published in November 2024.

Who Does The Offence Apply To?

- "... **large**, incorporated bodies and partnerships" including those formed outside the UK with a **UK nexus.**
- An **individual subsidiary or franchise** that meets the criteria.

How Is A "Large Organisation" Defined?

An organisation that meets **two out of the three** following criteria is defined as a "large organisation":

- more than 250 employees;
- more than £36 million turnover; and/or
- more than £18 million in total assets.

Where a parent company and its subsidiaries together meet two out of the three criteria above, **the group of companies** may be in scope of the offence.

Who Are "Associated Persons"?

- An **employee**; or
- an **agent**; or
- a **subsidiary**; or
- a person who otherwise **performs services** for/on behalf of the organisation.

What Are The Base Fraud Offences That Can Trigger A Failure To Prevent Fraud Offence?

There are nine **base fraud offences**^v (England & Wales);

- | | |
|---|--|
| 1. Cheating the public revenue (common law) | 5. Fraud by false representation (Fraud Act 2006) |
| 2. False accounting (Theft Act 1968) | 6. Fraud by failing to disclose information (Fraud Act 2006) |
| 3. False statements by company directors (Theft Act 1968) | 7. Fraud by abuse of position (Fraud Act 2006) |
| 4. Fraudulent trading (Companies Act 2006) | 8. Participation in a fraudulent business (Fraud Act 2006) |
| | 9. Obtaining services dishonestly (Fraud Act 2006) |

The **offence can also be triggered** by aiding, abetting, counselling, or procuring the commission of any of the listed offences.^{vi}

How Does Liability Attach To The Organisation?

The organisation may be **prosecuted** if the base fraud committed by an associated person:

- was intended to **benefit** the **organisation**;
- was intended to **benefit** the organisation's **clients**, to whom the associated person **provides services** for/on behalf of the organisation; or
- the **organisation's clients**, where the services are provided to **subsidiaries of those clients**.

The exception:

Where the organisation is the victim/intended victim of the base fraud.

How Does Liability Attach To A Subsidiary?

- If a subsidiary or franchise meets the criteria for the definition of a large organisation, it can be **directly liable** in its own right.
- If a base fraud is committed by an **employee of a subsidiary of a large parent organisation**, the subsidiary could be prosecuted for failure to prevent fraud, if the base fraud was intended to **benefit the subsidiary**.
- However, if the base fraud was intended to benefit the **parent organisation**, the latter could be prosecuted.

Does The Offence Apply To Individuals Too?

- **No** - the offence is a **corporate** one. The prosecution of an **individual** for the base offence is **not required** to prosecute an **organisation** for failure to prevent the base fraud.
- A prosecutor must prove to a **criminal standard** that a base fraud was attempted/committed.
- The person(s) who commits the base fraud may be prosecuted for it, whilst an organisation may be prosecuted for **failing to prevent** the fraud.

If An Employee Commits A Fraud In Their Private Life, Can The Organisation Be Held Liable?

If an associated person commits a base fraud offence that is **outside** of their capacity as an associated person, and relates to their **private/personal** life, then the organisation cannot be held liable.

Does The FTPF Offence Apply to Public Bodies?

Yes, public bodies, charities and other organisations are within scope if they meet the relevant criteria for a "large organisation".

Are SMEs Within Scope Of The Offence?

Contact us today to find out more
info@fraud-sentinel.com

fraud-sentinel.com

- They are **not** directly within scope.
- However, SMEs may be considered “associated persons” whilst they provide **services for/on behalf** of large organisations.

Does The FTFP Offence Have Extra-Territorial Reach?

- There is a requirement for a **UK nexus**.
- An associated person must commit a base fraud offence **under UK law**.
- This means that one of the acts which is part of the **underlying base fraud**, or the actual **gain/loss**, took place **in** the UK.
- If **no part** of the base fraud offence took place in the UK and there is **no actual loss/gain**, then there is **no UK nexus**.
- If a **UK-based employee** commits a base fraud offence, the relevant organisation could be prosecuted, **regardless** of where it is based.
- An **overseas-based** organisation could also be prosecuted if their employee/associated person commits a base fraud offence in the UK, or targets victims in the UK.

Are There Any Defences Available?

- If **prosecuted**, the organisation must prove to the court that it had reasonable fraud prevention measures **in place** when the fraud was committed, **or** that it was **not reasonable in all the circumstances** for the organisation to have any prevention procedures in place.
- The standard of proof is on the **balance of probabilities**.
- A **lack** of relevant preventive measures may be deemed reasonable in **some instances**.
- However, it is unlikely that a court will find the decision to not conduct a **risk assessment**, to be reasonable.
- Therefore, a risk assessment is **crucial**. If not conducted **thoroughly**, or not **reviewed and updated regularly**, an organisation may be unable to rely on it as part of its defence.

What Are The Penalties?

- A **criminal conviction** for the organisation.
- A **financial penalty**, with the court considering **all the circumstances** to decide the appropriate level of fine.

Are Deferred Prosecution Agreements (DPAs) Available For This Offence?

Yes, in **England and Wales** only.

The prosecutor will determine the **most appropriate way** in which to deal with an organisation, taking into consideration **factors** such as:

- The organisation’s willingness to **co-operate** with an investigation.

- Whether it makes a **full disclosure**.
- Whether it meets all the other **criteria** for a **DPA**.

What Are The Six Key Principles To Consider?

There are six principles that should inform an organisation's **fraud prevention frameworks**. They are intended to be "**flexible**" and "**outcome-focussed**" to reflect the diversity of circumstances that an organisation may find itself in.

1 - Top Level Commitment

- The **board, partners** and **senior management** should be committed to developing an **anti-fraud culture** with their organisation.
- The **responsibility** for fraud prevention and detection sits with the **most senior** leaders in the organisation.
- Senior management should take the **lead** in relation to fraud prevention by:
 - Committing to **training and resourcing** of the fraud prevention strategy.
 - Leading by **example**.
 - Encouraging a **speak-up culture**.
 - Clearly **communicating** across the organisation on fraud prevention.

Ensuring clear **governance structures** in relation to the fraud prevention framework.

2 - Risk Assessment

- Organisations need to **evaluate their exposure** to the **risk** of associated persons committing a base fraud offence(s) and making the organisation **liable**.
- Organisations must conduct a **comprehensive and documented** risk assessment of all the fraud risks relevant to the FTPF offence.
- Nominated risk owners should develop "typologies of risk" by considering the **fraud triangle** elements (opportunity, motivation, and rationalisation), factoring in **territorial scope** and drawing from various **information sources** about potential risk.
- The risk assessment should be reviewed at **regular** intervals, and more frequently if internal or external factors require it.
- A risk assessment that has **not** been regularly reviewed may **not** be considered by a court as **fit for purpose**.

3 - Proportionate Risk-Based Prevention Procedures

They must be **clear, practical, accessible**, and "effectively **implemented and enforced**".

Organisations should consider implementing the following:

- A fraud prevention plan that is **proportionate** to the risk and potential impact.
- Evaluate its **existing** compliance programme, financial reporting controls, and fraud prevention measures.

4 - Due Diligence

- Organisations must take a risk-based and proportionate approach to due diligence procedures in order to **mitigate** identified fraud risks.
- Organisations must **tailor** due diligence procedures to the fraud risks identified, rather than applying existing procedures designed to mitigate other types of risks.
- Due diligence should be conducted on associated persons using **technology**, and also in the **onboarding** of agents and the **contract management** process for suppliers.

- Consider the **sufficiency** of those existing measures and their **ability to prevent** each of the fraud risks identified in the risk assessment.
- Undertake **testing** of their fraud prevention measures and controls to determine the **effectiveness** of those controls and measures.

- Organisations should consider the **wellbeing** of staff and agents, to identify those who may be **vulnerable** to committing the base fraud offences because of issues such as stress, workload, etc.

5 - Communication

“Training and maintaining training are key.”

- Organisations should ensure that their fraud prevention **policies and procedures** are **communicated, embedded** and **understood** throughout the organisation.
- An organisation’s anti-fraud policy should be clearly **articulated** and **endorsed by leaders** across all levels within the organisation.
- Organisations should ensure that those who **provide services** for/on their behalf, are aware of and **understand** their fraud prevention policies.
- Training should be **targeted and proportionate** to the risk, with **specific** and detailed training delivered to those in the **highest-risk** positions and divisions within the organisation.
- Organisations should consider **integrating fraud messaging** into existing policies and procedures.
- Organisations may choose to **internally publicise** the outcome of investigations and sanctions.
- It is important for organisations to have **effective whistleblowing** procedures and mechanisms in place, to facilitate a **speak-up culture**.

6 - Monitoring and Review

Monitoring includes three elements:

- Implementation of measures to **detect fraud and attempted fraud**, and consideration of how existing measures can be extended to detect the base fraud offences.
- Having arrangements in place for the **investigation of suspected fraud** within the offence’s scope. Investigations should be **independent**, properly resourced, scoped and **fair** to all involved.
- **Monitoring the effectiveness of fraud prevention measures.** This may include financial controls, data collection on staff training for fraud prevention, and updates to due diligence procedures.

Do We Need To Make Any Changes To Our Compliance Programme?

YES! Your organisation only has until **1st September 2025** to be **fully compliant!**

Getting Ready: What Next?

- √ **Engage the board and senior management** on what is required from them, and the organisation as a whole, to ensure compliance.
- √ Identify **nominated risk owners**.
- √ **Create a fraud prevention plan**.
- √ Undertake a **comprehensive fraud risk assessment** for the organisation.
- √ Assess **existing fraud risk management frameworks**.
- √ Conduct **training** of employees at **all levels** on the FTPF offence, and on how to identify and report potential fraud.
- √ **Assess and update the whistleblowing framework**.
- √ **Update communications and training** to ensure awareness of how to report fraud-related concerns.
- √ **Seek external advice and support** with respect to the specific risks of your organisation.
- √ **Document all decisions** made in relation to the implementation of fraud prevention procedures.
- √ **SMEs** should revise risk assessments with the Guidance in mind. They can fall under the “associated person” definition and may be subject to **related requirements** by organisations.
- √ **Review internal investigations procedures** to ensure independence, adequate resourcing, capacity and expertise to investigate the base fraud offences.
- √ Do not rely on an **audit alone** to provide assurance about the appropriateness/effectiveness of your **controls**.

Get in touch with the Fraud Sentinel team, and we will be happy to discuss how we can help your organisation to get ready for the Failure to Prevent Fraud offence.

Key Contacts



Lloydette Bai-Marrow
Managing Partner
T +44 (0)208 058 3120
Lloydette@parametricglobal.co.uk
[LinkedIn](#)

Parametric Global Consulting
Info@parametricglobal.co.uk
[Website](#)
[LinkedIn](#)

Contact us today to find out more
info@fraud-sentinel.com

fraud-sentinel.com



Roberto di Cillo
Associate Consultant
[Profile](#)



**Cecilia Garcia
Podoley**
Associate Consultant
[Profile](#)



Andrew Clarke
Associate Consultant
[Profile](#)

References

-
- ⁱ Section 199 of the Economic Crime and Corporate Transparency Act 2023
- ⁱⁱ Guidance: Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud:
<https://assets.publishing.service.gov.uk/media/675c46ce0fb02bbe4853ef14/Failure+to+Prevent+Fraud+Guidance+-+English+Language+v1.4.pdf>
- ⁱⁱⁱ Economic Crime and Corporate Transparency Act 2023: <https://www.legislation.gov.uk/ukpga/2023/56/contents>
- ^{iv} Policy paper: Economic Crime and Corporate Transparency Act: failure to prevent fraud offence:
<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>
- ^v Schedule 13 of the Economic Crime and Corporate Transparency Act 2023
- ^{vi} Section 199(6)(b) of the Economic Crime and Corporate Transparency Act 2023