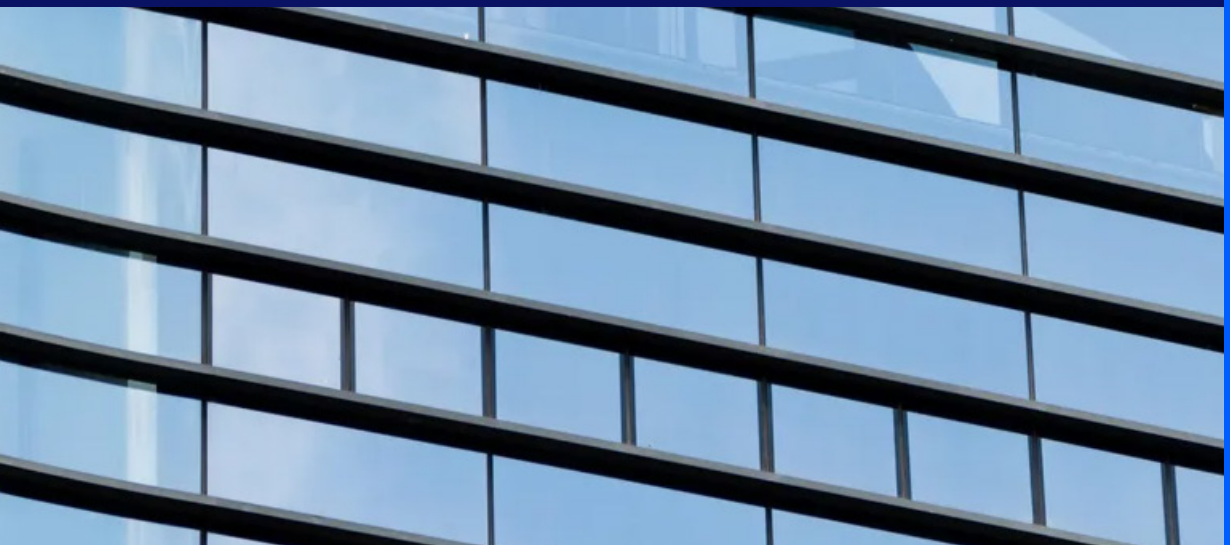
MOODY'S

Failure to Prevent Fraud

EBOOK



Chapter 1: Understanding the UK's Failure to Prevent Fraud Offence

The Failure to Prevent Fraud (FTPF) offence, introduced under the UK government's Economic Crime and Corporate Transparency (ECCT) Act 2023, represents a seminal moment in corporate law.

From September 1, 2025, large organizations can potentially be held liable if it is found that an employee, agent, or subsidiary commits fraud for the organization's benefit and the company cannot show it had "reasonable procedures" in place to prevent it.

The ECCT Act and the FTPF offence demonstrate an enhancement of corporate accountability for fraud. Under the FTPF offence, the burden has shifted: organizations accused of an offence need to prove they were proactive in preventing fraud—i.e., by having "reasonable procedures" in place—or face penalties, including unlimited fines.

IMPLICATIONS FOR RISK AND COMPLIANCE

Compliance in relation to fraud risk has become a strategic imperative, as Boards need to be confident that fraud risk management and prevention are embedded across an organization—from procurement and sales to HR and IT. The FTPF offence is designed to change corporate culture to think about and tackle fraud in a systemic way; for organizations to try and prevent it from happening in the first place—it is not just about punishing bad actors.

The offence applies to "large organisations," which is defined as those meeting two or more of the following criteria:

More than 250 employees	Annual turnover over £36 million	Assets over £18 million

That said, smaller companies may be indirectly affected if they act as "associated persons" to larger organizations. Indeed, as stated on the gov.uk website: "Under the offence, large organisations may be held criminally liable where an employee, agent, subsidiary, or other 'associated person,' commits a fraud intending to benefit the organisation." This may lead to smaller businesses seeking to implement anti-fraud procedures too.

As liability can extend to associated persons—including, for example, contractors and suppliers who perform services on behalf of an organization—businesses may need to widen their fraud risk management framework. The "associated persons" dynamic underscores the importance of comprehensive and robust due diligence and ongoing monitoring to mitigate exposure to liability.

MOODY'S

Chapter 2: Fraud prevention in the UK and beyond

The UK's new offence has significant implications for non-UK businesses, especially those with any connection to the UK. The FTPF offence can apply to companies who are not based in the UK if there is a sufficient UK nexus to the fraudulent activity. For example: if the fraud involves a UK customer, supplier, or subsidiary; the fraudulent conduct affects UK markets or victims; or the company operates in the UK or has UK-based employees or agents.

Moreover, it is a strict liability offence, meaning a company can be held liable even if it did not benefit from the fraud or was unaware of it.

The key defence is to show that the company had what is known as "reasonable procedures" in place to prevent fraud.

This is not an exhaustive list, but examples of reasonable procedures might include:

- Updating or implementing anti-fraud policies
- Training staff and agents
- Conducting screening for risk assessment
- Ongoing audits

"Under the new 'Failure to Prevent Fraud' offence, an organisation may be held liable where a specified fraud offence is committed by an employee or agent acting on the organization's behalf. This increases the importance for government and corporate vigilance on the web of direct and indirect risks they face from financial crime."

Ted Datta, Head of Industry Practice Group – Europe & Africa at Moody's

Chapter 3: What may be considered “Reasonable Procedures”?

The key defence under the FTPF offence is to show that the organization had reasonable fraud prevention procedures in place. This might mean tailoring controls to the specific risks of a sector, geography, and business model when it comes to fraud.

6 PRINCIPLES

The UK Government outlines six principles to help establish a framework of reasonable procedures:

1. Top-level commitment
2. Risk assessment
3. Proportionate procedures
4. Due diligence
5. Communication and training
6. Monitoring and review

These are not designed to be checkboxes but rather help organizations develop the foundations for a culture of fraud prevention.

EXAMPLES AND POTENTIAL PITFALLS

“Top-level commitment” could mean demonstrating CEO endorsement of a fraud risk management program, but also visible leadership, resource allocation, and integration of fraud risk into strategic decision-making.

“Communication and training” could mean establishing regular internal communications networks and channels to discuss and share findings related to fraud risk. This could include training and development requirements to keep staff alert to fraud risk and suspicious activity.

If reasonable procedures means tailoring a risk management control framework for a business, this is where companies could face a potential pitfall. Relying on a generic fraud prevention policy or repurposing an anti-bribery framework may not be sufficient, as fraud prevention may require different bespoke, dynamic, and data-driven controls.

Chapter 4: Transformation of the SFO and global fraud-related regulation

The UK's Serious Fraud Office (SFO) is undergoing a transformation. Under its new strategy, dubbed "SFO 2.0," the agency is focusing on faster investigations, higher conviction rates, and greater use of Deferred Prosecution Agreements (DPAs).

COLLABORATIVE ENFORCEMENT MODEL

DPAs may help a company avoid prosecution if they admit wrongdoing, cooperate fully, and implement reforms. Thus, DPAs may be a powerful tool for those who act early and transparently. For companies, this may mean self-reporting and remediation become strategic advantages.

THE GLOBAL LANDSCAPE OF FRAUD REGULATION

The UK is not acting in isolation by adapting its approach to fraud and strengthening anti-fraud-related regulation. Around the world, regulators are reviewing and tightening frameworks related to preventing corporate fraud.

Singapore's Shared Responsibility Framework mandates banks and telcos implement real-time fraud surveillance and customer alerts to enhance consumer protection.

The EU's PSD3 and PSR proposals expand liability for payment service providers in fraud cases.

The ISO 37003:2025 standard offers a global framework for fraud control management systems, covering everything from prevention to response.

These developments appear to reflect a broad consensus that fraud is not only a financial risk—it's a systemic threat to trust, stability, and economic integrity. As digital transactions grow, so do opportunities for bad actors. Regulators across different jurisdictions are responding by asking for greater accountability and transparency from organizations in helping them address the threat of fraud.

For multinational firms, this means navigating a patchwork of evolving rules. But it also presents an opportunity: those who invest in robust, globally aligned fraud risk management and prevention controls may be able to turn compliance into competitive advantage.

Chapter 5: Due diligence in the age of AI and Shell Companies

Fraudsters are evolving—and so must defences. The rise of AI-powered scams, from deepfakes to synthetic identities, is making fraud harder to detect and easier to scale. Meanwhile, vehicles like shell companies can be exploited to obscure ownership and facilitate illicit financial flows.

MODERN THIRD-PARTY RISK MANAGEMENT AND DUE DILIGENCE TECHNIQUES

Modern third-party risk management and due diligence can be critical components of a robust fraud risk management framework, both at the onboarding stage and throughout the lifecycle of a third-party relationship.

At onboarding, organizations can implement comprehensive due diligence processes to help assess overall risk, as well as ownership structures and the reputational standing of a third-party entity. These processes may include leveraging data analytics, adverse media screening, and beneficial ownership verification to identify potential red flags.

Ongoing monitoring can support continuous risk assessments, including periodic re-evaluations or a perpetual approach—also known as perpetual KYC (pKYC)—based on changes in business operations, geography, regulatory landscape or other factors.

Integrating automated tools and dynamic data feeds can support the ability to detect anomalies, emerging and connected risks earlier. By embedding these practices into a fraud risk management strategy, organizations may be able to proactively mitigate exposure to fraud, as well as other third party-related risks.

Chapter 6: Strategic questions for Boards and Executives

BOARDROOM CONSIDERATIONS

When addressing the issues of fraud, control frameworks, and reasonable procedures, directors can ask key questions of their organization, such as:

- Are we treating fraud as a strategic risk, rather than a compliance issue?
- Do we understand our exposure across subsidiaries, agents, and third parties?
- Are we using technology to help detect fraud risk?
- Is our culture one of integrity?

Chapter 7: How can Moody's help with fraud risk management?

Moody's offers a suite of tools that assist organizations with proactively identifying and mitigating risks across their third-party networks. At the heart of these solutions is the ability to help verify information about individuals and entities before they are onboarded—and then screening for potential risks once connected via a counterparty network.

By leveraging Moody's global database of more than 580 million entities, businesses can potentially uncover hidden ownership structures, detect links to sanctioned individuals, and flag associations with adverse media or previous fraud cases. Tools like Moody's Shell Company Indicator and Adverse Media Screening can also help organizations by surfacing red flags and dynamic alerts tied to evolving risk profiles.

For due diligence and beyond, Moody's also supports ongoing fraud risk management through its Maxsight™ platform—a unified risk management platform designed to integrate seamlessly into workflows.

Maxsight™ supports organizations by centralizing data from disparate sources, automating screening, and generating reports that can highlight interconnected risks across a counterparty network. This is particularly valuable for large, complex organizations navigating a global customer base and tiered supply chains.

MOODY'S

MOODY'S

CONTACT INFORMATION

Americas
+1.212.553.1658
clientservices@moodys.com

Europe
+44.20.7772.5454
clientservices.emea@moodys.com

Asia (Excluding Japan)
+85.2.2916.1121
clientservices.asia@moodys.com

Japan
+81.3.5408.4100
clientservices.japan@moodys.com

REFERENCES

New failure to prevent fraud guidance published
Economic Crime and Corporate Transparency Act 2023: Guidance to ...
ISO 37003:2025 - Fraud control management systems — Guidance for ...
New Era of Fraud Prevention: Global Regulations Demand Accountability ...
Top Fraud Trends and Predictions for 2025 – And How Will the Industry ...
Fraud Strategy: stopping scams and protecting the public (accessible)
Failure to Prevent Fraud' and Exposure for Non-UK Businesses
UK's new failure to prevent fraud offence and how it impacts non-UK ...