Bottomline

THE UK FAILURE TO PREVENT FRAUD OFFENCE

Act Now to Protect Your Organisation and Comply with New Regulations.

bottomline.com

Introduction

By September 1, 2025, organisations must comply with the UK's Failure to Prevent Fraud offence, introduced under the Economic Crime and Corporate Transparency Act (ECCTA) 2023[1]. This regulation holds large[2] organisations accountable for failing to prevent fraud committed by their employees, agents, contractors, or other "associated persons" acting for the organisation's benefit, whether directly or indirectly.

The offence applies to fraud as defined in the Fraud Act 2006[3], including insider fraud, where individuals abuse their trusted positions, such as employees, agents, contractors, or subsidiaries. Insider fraud is particularly concerning because it exploits sensitive data, undermines internal controls, and harms organisational integrity, making it a critical focus of fraud prevention efforts.

The legislation applies not only to organisations based in the UK but also to foreign organisations with employees or victims in the UK, which must consider its potential impact. Notably, organisations may still be held liable even if senior management is unaware of the fraudulent actions.

The message is clear: Fraud prevention demands proactive measures. Organisations must prioritise risk assessments, secure high-risk internal systems, monitor privileged access, and implement regular training. By addressing insider threats as part of these efforts, they not only mitigate fraud risks but also demonstrate compliance, protect their reputation, and earn stakeholder trust.

Non-compliance could lead to unlimited fines, legal exposure, and irreparable reputational damage. To comply, organisations must demonstrate reasonable fraud prevention procedures. The UK government published guidance on November 6, 2024, emphasizing six core principles for compliance:

1. **Risk Assessment:** Identify and address key fraud risks.
2. **Proportional Procedures:** Align measures with organisational size and complexity.
3. **Top-Level Commitment:** Leadership must actively support anti-fraud efforts.
4. **Due Diligence:** Vet employees, agents, and third parties thoroughly.
5. **Communication and Training:** Embed fraud prevention into company culture.
6. **Monitoring and Review:** Continuously improve fraud controls.

---

1 The ECCTA 2023 is the overarching legislation that modernizes and strengthens the UK's approach to tackling economic crime, including introducing corporate accountability mechanisms like the Failure to Prevent Fraud offence.

2 An organisation is considered large if it meets two or more of the following criteria: more than 250 employees, more than £36 million turnover, or more than £18 million in total assets.

3 Fraud Act 2006 defines the offences that constitute fraud (including internal fraud) and forms the basis for individual criminal liability. Failure to Prevent Fraud offence (ECCTA 2023) extends liability to organisations for failing to prevent Fraud Act offences by their associated persons.

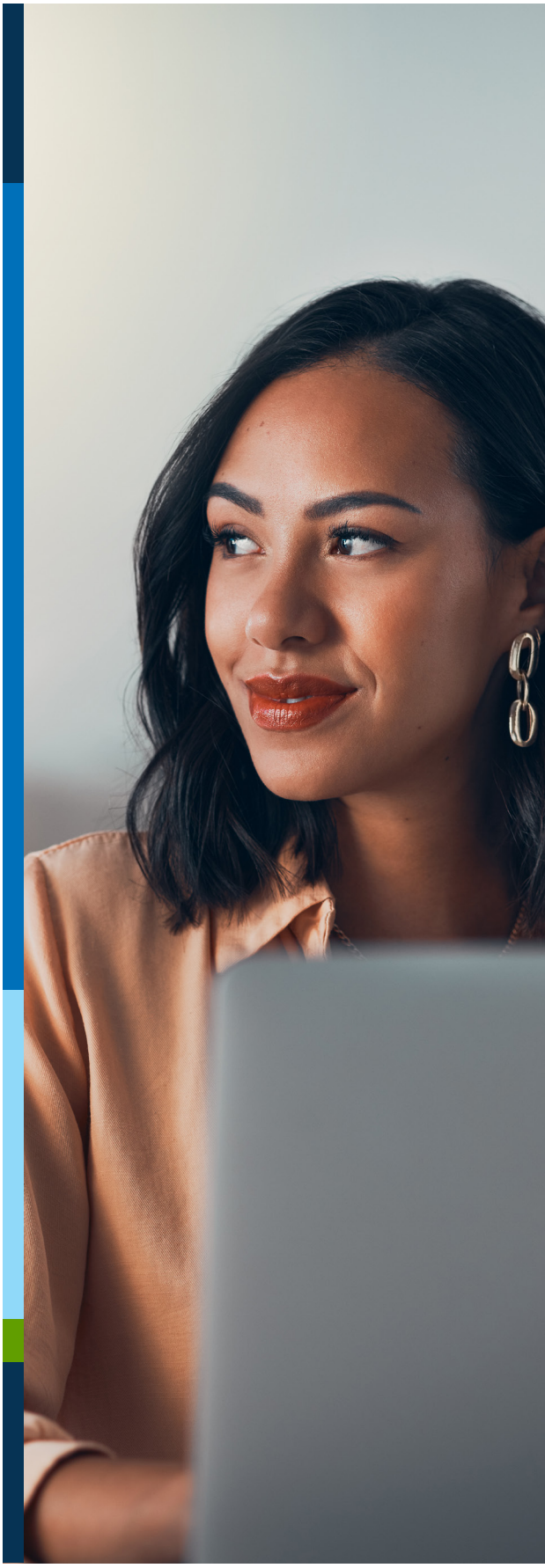
4 https://www.gov.uk/government/news/new-failure-to-prevent-fraud-guidance-published

The Challenges of Compliance

Preparing for the new offence is a significant challenge, with four critical hurdles organisations must overcome:

1. **Regulatory Pressure:** Scrutiny is intensifying, with regulators demanding robust fraud prevention measures and detailed documentation. Falling to prevent fraud could lead to severe penalties and reputational damage.
2. **Insider Fraud Complexity:** Differentiating between malicious intent and routine employee actions becomes complex when legitimate system commands and processes are used by all staff. Advanced and adaptive tools are crucial to identify subtle patterns and anomalies that signal fraudulent behaviour without disrupting normal operations.
3. **Resource Limitations:** Many organisations struggle to meet compliance requirements due to limited budgets and in-house expertise, making it hard to keep pace with expectations.
4. **Demand for Transparency:** Regulators and auditors require clear, comprehensive records of fraud prevention measures. Failure to demonstrate compliance could expose organisations to financial and legal risks.

To succeed, organisations must rethink their approach to insider threats, embracing scalable technologies and adopting a proactive compliance mindset to counter these challenges.



Leveraging Insider Threat Technology

Insider threat technology is no longer optional - **it's essential.** The guidance under the Failure to Prevent Fraud offence highlights technology as a critical enabler of effective fraud defences.

Outdated methods create a dangerous false sense of security. Fraud tactics are evolving rapidly, bypassing traditional defences. Modern solutions, like Bottomline's Insider Threat Management (ITM), leverage advanced detection capabilities to stay ahead of these threats. By adopting these solutions, organisations not only reduce their risk of penalties but also demonstrate a proactive commitment to compliance, building trust with regulators and stakeholders.

Driving Compliance and Fraud Prevention with Bottomline

Bottomline's Insider Threat Management (ITM) accelerates investigations, enabling organisations to reduce costs by streamlining processes and resolving fraud cases with greater efficiency. Equipped with advanced features to support compliance with the Failure to Prevent Fraud offence, Bottomline delivers proactive fraud detection and effective insider threat management.

Key Features and Benefits

1

Record and Replay Technology

How It Works: Captures and replays user activity within sensitive internal applications, offering complete visibility into user actions involving critical data. This feature enables the detection of fraud in sensitive internal systems, such as ERP, CRM, and financial platforms, by providing screen-by-screen replays of user activity.

Why It Matters: Speeds up investigations, simplifies audits with precise and irrefutable visual evidence, and provides real-world scenarios for effective training. It helps organisations address the limitations of traditional audit trails in corporate applications, which often lack comprehensive details on user access to customer data—especially for inquiries that leave no trace.

Compliance Impact: Ensures alignment with the law's monitoring and review requirements.

2

Real-Time Fraud Detection

How It Works: Offers 24/7 monitoring of employee access to sensitive internal systems, detecting and flagging anomalies such as unauthorized access, after-hours logins, irregular inquiries on sensitive data, suspicious modifications, excessive data downloads, and privilege escalation attempts.

Why It Matters: Detects and stops fraudulent activity in real-time before it escalates into significant breaches.

Compliance Impact: Demonstrates proactive fraud prevention and monitoring to regulators, reducing the risk of penalties or reputational damage.

3

Proportional Risk Monitoring

How It Works: Implements fraud prevention measures tailored to the organisation's size, industry, and specific risk profile.

Why It Matters: Ensures fraud prevention efforts are both effective and appropriate, addressing the unique risks the organisation faces without unnecessary overreach.

Compliance Impact: Demonstrates a reasonable, risk-based approach to regulators, fulfilling legal obligations, protecting resources, and safeguarding sensitive data while reducing liability.

4

End-to-End Fraud Management

How It Works: Consolidates fraud detection, case management, and reporting into a unified and efficient platform. Built-in controls for detecting suspicious activity can be correlated with information ingested from other systems.

Why It Matters: Simplifies compliance and investigation workflows, boosts operational efficiency, ensures a robust audit trail, and provides comprehensive documentation of fraud investigation and prevention efforts.

Compliance Impact: Demonstrates strong control measures, enhances audit readiness, and aligns with regulatory expectations under the Failure to Prevent Fraud offence.

5

Regulatory Alignment - Compliance meet Privacy

How It Works: Provides indisputable screen-by-screen evidence and case documentation tailored to meet compliance standards, while respecting employee privacy by excluding personal communications, (e.g., emails, chats) or internet whereabouts.

Why It Matters: Strikes a balance between protecting employee privacy rights and safeguarding customer data while ensuring compliance with regulatory demands. Enhances audit readiness, promotes transparency, and demonstrates accountability to regulators.

Compliance Impact: Aligns fraud prevention practices with GDPR and the requirements of the Failure to Prevent Fraud offence, demonstrating proactive compliance to regulators while building customer trust and preserving employee privacy.

Take the Next Step

The Failure to Prevent Fraud offence presents both a challenge and an opportunity for organisations to enhance their fraud defences. With the offence coming into force on September 1, 2025, it is crucial for organisations to proactively implement compliance measures well in advance to ensure readiness.

Partner with Bottomline to:

Strengthen insider threat defences using advanced technology.

Achieve compliance with the latest regulations.

Protect your organisation's reputation and build stakeholder trust.

Contact Bottomline today to learn how we can help you prepare for the Failure to Prevent Fraud offence and ensure your organisation stays ahead of the curve.

Contact Us

Bottomline

REV US011625LM

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com