Creating a safer
Cambridgeshire

2025/26 Annual Fraud Report

28 May 2026

Jon Lee, CFO and Director of Resources

1. Introduction

1.1 The Constabulary produces an annual report setting out the actual and suspected fraud against the organisation. This report provides the overview for the awareness of Chief Officers, senior management, and the Joint Audit Committee (JAC).

2. Fraud Against the Constabulary

2.1 In respect of cases of fraud against the organisation based on conduct and anti-corruption intelligence for 2025/26 there have been 18 cases of alleged fraud – an increase on the prior year where 6 alleged cases and/or reports were identified.

2.2 There are 2 conduct cases, and 5 intelligence reports that relate to alleged 'key-jamming'. In these cases, individuals have used software or physical devices to appear working when they are not.

2.3 Of the cases related to key-jamming, one conduct case has led to a dismissal. The others were either dealt with by line management or were No Case to Answer.

2.4 The further 2 conduct cases and 9 intelligence reports include allegations relating to officers/staff claiming overtime hours not worked or not working their required duties, receiving shift allowance payments when not entitled, falsifying a record to obtain an academic qualification as part of their employment, potential theft of property destined for disposal and claiming excessive fuel allowance.

2.5 The 3 live conduct cases from 2024/2025 relating to allegations of conducting their business interest role during policing hours, dishonesty on a vetting application and failure to disclose details of a relationship during their integrity

health check have concluded as No Case to Answer, with one still live and awaiting conclusion.

2.6 One intelligence report relates to fraud in the next reporting period 2026/27. It relates to an officer taking annual leave without booking it on force systems. This report is currently live. No further conduct cases or intelligence reports have been recorded.

2.7 Intelligence reports are submitted to the Anti-Corruption Unit from a range of sources. This may include members of the public, line managers, peers, through proactive analysis of data (such as work phone usage, overtime) or anonymous reporting.

2.8 The number of cases relating to suspected fraudulent activity has risen since last year, partially due to proactive analysis that has taken place. However, it is a low level of suspected fraudulent activity with one conduct case leading to a dismissal. Although at the time of writing some of the alleged cases remain ongoing.

3. Controls / Procedures

3.1 Given the low level of suspected fraud within the Constabulary no immediate changes have been made or are required to the controls and procedures at this time. Controls in place in respect of fraud include:

- A **Central Fraud Register** is maintained by the Head of Finance in conjunction with the Professional Standards Department (PSD). During 2025/26 the register has continued to capture all alleged and suspected fraud cases, including conduct and intelligence matters, with outcomes and status updated as investigations progress. The register is reviewed periodically to identify themes, trends and control implications and is aligned to the fraud risk assessment. A summarised version of the register is included at Appendix 1.

  During 2025/26 the Constabulary expanded its **Fraud Risk Assessment** to reflect new and emerging risks arising from changes in working practices and operational activity. These included risks associated with working time misrepresentation in remote working environments, theft or misuse of property and evidence at crime scenes, and the inappropriate retention or resale of police issued uniforms and equipment.

  While these risks are assessed as having a low likelihood of occurrence, some carry potentially significant reputational or public confidence impacts. Existing preventative and detective controls – including management oversight, body-worn video, audit and inventory controls, and clear standards of professional behaviour – are considered sufficient to mitigate these risks to a tolerable level, with ongoing monitoring in place to ensure controls remain effective

- **Anti-Fraud Training** – fraud awareness eLearning continues to be mandatory for staff in higher risk functions including finance, payroll, HR, procurement, business support and uniform stores. Completion monitoring is undertaken as part of normal training governance arrangements, with compliance followed up locally where required. Training remains a standard requirement for new starters in these areas of the Constabulary. On 31 March 2026, completion rates across core finance and transactional teams remained high at 85%.

- Reports have been extracted by the Anti-Corruption Unit (ACU) to enable the finance team to **review declarations of interes**t against accounts payable (AP) data. During 2025/26 this work has continued on a periodic basis. A small number of matches have been reviewed by Finance and PSD as part of routine assurance activity; none required escalation to a formal fraud investigation. The process continues to mature alongside wider data led fraud prevention work.

- The ACU and Payroll team continue to undertake joint working to share **expenses data** and **overtime claimant data** where the ACU review the information to identify fraud and/or financial vulnerability concerns. Expenses data is being received monthly by the ACU and is being reviewed for high claimants and individuals with repeatedly rejected expense claims.

- The **National Fraud Initiative (NFI)** national exercise which is carried out every two years using data matching/analytics to compare different datasets across participating organisations. The Constabulary is due to next undertake the exercise in September 2026. The NFI helps to identify potentially fraudulent claims, errors and overpayments. The NFI is conducted in England under the Local Audit and Accountability Act 2014.

- The BCH Combined Financial Regulations includes the **Fraud Prevention, Anti-Bribery and Corruption Strategy** which all officers and staff are required to adhere. Cambridgeshire Constabulary includes this in local Force Financial Instructions which are refreshed annually and the CFO highlights the requirement to adhere to these regulations and instructions in letters which go to all budget managers.

4. 2025/26 Internal Audit

4.1 The 2025/26 internal audit programme included a BCH advisory audit on the steps needed to progress the fraud risk framework to meet the requirements of the corporate liability offence of Failure to Prevent Fraud (FTPF) within the Economic Crime and Corporate Transparency Act 2023 (ECCTA). The Act creates a corporate offence of failing to prevent fraud when an ‘associated person’ commits a specified fraud offence, which is intended to benefit the ‘relevant body/organisations’. The only potential defence is for the force to

demonstrate that it has reasonable procedures in place to prevent such a fraud from being committed.

4.2 Appendix 2 provides an overview of the ECCTA for Chief Officer awareness and consideration.

4.3 The audit identified that the Constabulary has a good base to build from identifying further enhancements that can be made to the existing fraud arrangements. These improvements will be progressed in 2026/27 and include:

a) Ensuring top level commitment to the ECCTA – this report and the arrangements the Constabulary has in place will be reported to the Chief Constables Force Executive Board in June 2026 and will also be reported to the Police Accountability Board of the PCC.

b) Refinement of the Fraud Risk Assessment to:

    a. identify, articulate, assess and clearly define the types of fraud the force may be at risk from as a beneficiary in line with the requirements of the FTPF offence; and

    b. regularly update and review the Fraud Risk Assessment to enable new and emerging risks to be identified and responded to appropriately and ensure adequate periodic objective oversight.

c) Reviewing procedures to ensure they cover preventing fraud by persons associated with it, proportionate to the risks it faces and to the nature, scale and complexity of the forces' activities.

d) Identifying their associated persons and following identification of associated areas of risk, in line with the failure to prevent fraud offence', will clearly articulate the respective due diligence procedures undertaken.

e) Reviewing the online training to ensure that the training covers all required areas.

f) Developing and implementing a range of measurement criteria to be monitored and reported periodically to the Joint Audit Committees (JAC).

g) Updating the Combined Financial Regulation policy to include reference to the Economic Corporate Crime and Transparency Act (ECCTA).

5. Fraud Risk Assessment

5.1 The Constabulary developed a fraud risk register in 2023/24 to capture the key areas of potential fraud, understand the level of risk, exposure and potential impact and map any controls and mitigations in place. Further enhancements to the control environment in relation to fraud are kept under review as part of the monitoring processes. The fraud risk register is maintained by the Head of Finance and reported at six-monthly intervals to the Constabulary's Risk Review Board, with emerging risks, control effectiveness and required actions monitored as part of the wider corporate risk framework.

5.2 The current Fraud Risk Register is provided at Appendix 1.

6. Recommendation

6.1 The JAC is asked to note the contents of the report.

APPENDIX 1 Fraud Risk Register Summary

Ref	Risk Area	Risk Summary	Control Summary	Residual Risk	Treatment Approach	Risk Owner	Key Assurance / Commentary
1	Payroll – Overtime	Risk of false or inflated overtime claims	Pre-authorisation, manager review, PSD monitoring	14 (Med-High)	Treat	PSD / HR	Ongoing review of overtime controls and enhanced reporting
2	Payroll – Expenses	Ineligible or inflated expense claims	Manager checks, receipt validation, payroll sampling	16 (High)	Treat	Finance / HR	Sampling identifies errors; reliance on manager scrutiny remains a weakness
3	Payroll – Allowances	Allowances paid when criteria no longer met	Annual payroll review	10 (Medium)	Tolerate	Payroll	Identified through annual checks; low materiality impact
4	Fleet	Misuse of vehicles for personal use	Policy refresh, vehicle tracking audits	6 (Low-Med)	Tolerate	Fleet	Monitoring has reduced likelihood; low financial impact
5	Fleet	Misuse of fuel cards	Allocation controls, audit checks	3 (Low)	Tolerate	Fleet / Finance	Strong controls; no known cases
6	Assets (ICT)	Theft or misuse of ICT equipment	Asset tracking, audits, comms	7.5 (Medium)	Tolerate	ICT / Line Mgmt	Risk reduced post-agile working adjustments
7	Estates / Facilities	Personal use of facilities (e.g. charging, equipment)	Policy, periodic checks	15 (High)	Treat	Estates	Cultural acceptance increases likelihood; policy tightening required
8	Procurement / Travel	Misuse of hotel booking system	Approval via BSU, restricted access	6 (Low-Med)	Tolerate	BSU	Strong approval controls in place
9	Estates / Contractors	Contractors undertaking private work	Vetting and checks	6 (Low-Med)	Tolerate	Estates	Low likelihood; no reported cases
10	Finance Controls	Misuse of credit cards, petty cash, trade accounts	Reconciliations, audits, independent review	6.25 (Low-Med)	Tolerate	Finance	Controls generally effective; some gaps in card control ownership
11	ICT / Cyber	Cyber attack / ransomware	Security controls, training, monitoring	10.5 (Medium)	Treat	ICT	Regular audit and high organisational focus
12	Property / Evidence	Fraud in cash handling / property process	CCTV, audits, segregation of duties	9 (Medium)	Tolerate	Property / Finance	Risks mainly at point of seizure rather than storage
13	Finance	Petty cash misuse	Supervisor approval, receipts	10.5 (Medium)	Tolerate	Finance	Use decreasing; low value exposure
14	Treasury	Diversion of funds during transfers	Dual controls, segregation, audit	3.5 (Low)	Tolerate	Finance	Strong segregation reduces risk significantly
15	Finance	Improper debt write-off	Supervisor approval, audit trails	3 (Low)	Tolerate	Finance	Low risk due to oversight and thresholds
16	Finance	Credit card fraud (external)	PIN controls, audits	5.25 (Low)	Tolerate	Finance	Low limits and active monitoring reduce exposure
17	Procurement	Payment for goods/services not received	PO / GRN / budget holder checks	8.75 (Medium)	Treat	Finance / Procurement	Risk remains where segregation is limited
18	Procurement	Fake supplier setup	Supplier verification, quote requirements	4.5 (Low)	Tolerate	Procurement	Strong onboarding and validation controls
19	Contract Management	Paying for undelivered services	Contract management, budget review	6.25 (Low-Med)	Tolerate	Budget Holders	Higher exposure in low-value contracts
20	Payroll	Non-repayment of advances/overpayments	Recovery processes, invoicing	5 (Low)	Tolerate	Payroll	More debt-related than fraud; low frequency
21	Procurement	Personal purchases via procurement routes	PO controls, approvals	7.5 (Medium)	Tolerate	Finance / Budget Holders	Limited access reduces exposure
22	Governance	Coercion of senior staff	Vetting, audit, proposed training	8 (Medium)	Treat	SLT	Low likelihood but high impact risk
23	Workforce	Time fraud (e.g. simulated activity)	Manager oversight, monitoring	10.5 (Medium)	Tolerate	HR / PSD	Emerging risk; controls evolving
24	Operational	Theft at crime scenes	BWV, audits, supervision	6.75 (Low-Med)	Tolerate	PSD / Ops	Serious impact but rare occurrence
25	Stores / Uniform	Sale or misuse of police-issued items	Inventory control, audits, monitoring	12 (Medium-High)	Tolerate	Stores / PSD	Reputational risk higher than financial

APPENDIX 2
(*note this summary has been produced using co-pilot from the Home Office guidance document prepared in November 2024*)

Economic Crime and Corporate Transparency Act (ECCTA) Executive Summary for Chief Officers

The offence of failure to prevent fraud fundamentally changes the risk landscape for large organisations. **Leadership, evidence and culture** will determine exposure. Chief Officers should treat this as a priority compliance and governance issue requiring visible ownership, structured assurance, and sustained oversight.

Purpose and Context

This guidance explains the new **corporate criminal offence of failure to prevent fraud**, introduced under the **Economic Crime and Corporate Transparency Act 2023** and effective from **1 September 2025**. The offence is designed to strengthen accountability by making large organisations criminally liable where fraud is committed by an associated person **intending to benefit the organisation or its clients**, and the organisation did not have **reasonable fraud prevention procedures** in place.

The offence represents a significant shift from previous arrangements: organisations can be prosecuted **even where senior leaders had no knowledge of, or involvement in, the fraud**. The statutory defence is the existence of reasonable prevention procedures. Chief Officers therefore have a critical leadership and governance role in ensuring organisational readiness.

1. Organisations in Scope

The offence applies **only to large organisations**, defined as incorporated bodies or partnerships that meet **two or more** of the following criteria (in the financial year preceding the fraud):

- More than **250 employees**
- Turnover exceeding **£36m**
- Total assets exceeding **£18m**

Key points for Chief Officers:

- The test applies at **group level**, including subsidiary undertakings, regardless of where they operate geographically.
- Subsidiaries may be prosecuted **in their own right**, or a **parent organisation** may be prosecuted where fraud by a subsidiary employee was intended to benefit the parent.
- Some public sector bodies (including those created by statute, such as NHS trusts and incorporated local authorities) may be in scope.

Although smaller organisations are not directly caught, they may be treated as **"associated persons"** when providing services to large organisations and may therefore be subject to increased contractual and assurance requirements.

2. Nature of the Offence

An organisation commits the offence where:

1. An **associated person** (employee, agent, subsidiary or other person providing services for or on behalf of the organisation) commits a specified **base fraud offence**; and
2. The fraud was committed **with intent to benefit** the organisation or its clients; and
3. The organisation did **not** have reasonable fraud prevention procedures in place.

Importantly:

- The organisation does **not** need to receive any actual benefit; *intended benefit* is sufficient.
- The fraudster's main motivation may be personal gain – the offence still applies if the organisation was also intended to benefit.
- Organisations are **not liable** where they are the victim or intended victim of the fraud.

Base fraud offences include fraud under the Fraud Act 2006, false accounting, fraudulent trading, cheating the public revenue, and equivalent offences in Scotland and Northern Ireland.

A UK nexus is required: at least one part of the fraud, or the gain or loss arising from it, must occur in the UK.

3. Enforcement, Penalties and Exposure

The offence may be prosecuted by the CPS, SFO or equivalent prosecuting authorities across the UK. Prosecution can proceed:

- Even if the individual fraudster is not prosecuted, provided the base fraud can be proven.

On conviction:

- Organisations face unlimited fines (subject to sentencing principles).
- Courts will consider the impact of fines on public and charitable functions for public bodies.
- In England and Wales, the offence is eligible for **Deferred Prosecution Agreements** (DPAs).

The presence, quality and operation of fraud prevention procedures will be a **central focus of investigations**, including where organisations self-report.

4. Defence: Reasonable Fraud Prevention Procedures

The **only statutory defence** is that the organisation had reasonable fraud prevention procedures in place, or that it was unreasonable to expect such procedures.

The burden of proof rests with the organisation, on the **balance of probabilities**.

What is “reasonable” is **context-specific** and determined by the courts, but the guidance sets out six core principles forming the expected framework:

1. **Top-level commitment**
   - Clear leadership from boards and senior management
   - Active ownership of fraud risk and prevention
   - Promotion of an anti-fraud culture, even where this conflicts with short-term performance pressures

2. **Risk assessment**
   - Documented, dynamic assessment covering frauds intended to benefit the organisation or its clients
   - Consideration of opportunity, motive and rationalisation (the fraud triangle)
   - Inclusion of supply chains, subsidiaries, agents and emergency scenarios

3. **Proportionate, risk-based procedures**
   - Controls aligned to the organisation’s size, complexity and risk profile
   - Use of existing controls where effective, but without assuming regulatory compliance is sufficient
   - Clear documentation where controls are not introduced for specific risks

4. **Due diligence**
   - Risk-based checks on employees, agents, contractors and subsidiaries
   - Strong contractual terms with associated persons
   - Enhanced scrutiny for mergers, acquisitions and partnerships

5. **Communication and training**
   - Clear internal and external messaging on zero tolerance of fraud
   - Role-specific training, particularly for high-risk functions
   - Accessible and trusted whistleblowing arrangements

6. **Monitoring and review**
   - Ongoing testing of controls and training effectiveness
   - Learning from audits, investigations and whistleblowing
   - Regular review by senior leadership, with escalation to boards as appropriate

It will rarely be considered reasonable **not even to have conducted a risk assessment**.

5. Strategic Implications for Chief Officers

For Chief Officers, this offence elevates fraud prevention to a **board-level statutory risk**, comparable to bribery and tax evasion.

Key implications:

- Fraud risk arising from *benefiting the organisation* must be explicitly addressed – not just fraud against the organisation.
- Reliance on audit, regulation or general financial controls alone is insufficient.
- Group structures, subsidiaries, and third-party delivery models require particular attention.
- Decisions, risk tolerances and exceptions must be **documented and defensible**.

In practice, organisations should ensure that fraud prevention frameworks are fully integrated into governance, risk management and assurance structures ahead of September 2025.