Fraudfinder LTD
71-75 Shelton St
London
WC2H 9JQ
United Kingdom

Email: alexander@fraudfinderai.com

Fraudfinder Fraud Policy

1. Purpose and Commitment

Fraudfinder is committed to preventing, detecting, and responding to fraud in all its forms, including fraud *detected* through our platform and fraud *perpetrated against* our business. As a fraud detection technology provider, maintaining integrity and trust is central to our business model.

---

2. Definitions

For the purposes of this policy, **fraud** refers to:

- Any intentional deception, misrepresentation, or abuse that causes financial or reputational harm to **Fraudfinder**
- Internal misconduct, including false expense claims, data falsification, or collusion with third parties
- Misuse of the platform (e.g., fake trial accounts, adversarial inputs, or unauthorised access)
- Client-side deception *only* where it constitutes a breach of terms (e.g., misuse of API, breach of fair usage)

---

3. Policy Statement

Fraudfinder has a **zero-tolerance policy** toward any form of fraud, whether committed by users, clients, employees, suppliers, or third parties. We actively **monitor, investigate, and act** on suspected cases and expect all stakeholders to report suspicious behaviour.

---

4. Fraud Prevention Measures

Fraudfinder maintains a layered prevention model:

For Clients / End Users:

- Robust AI-based detection models trained on diverse real and synthetic datasets
- Multi-layered fraud signals, including visual, structural, and behavioural checks
- Watermark, metadata, and font forensics for document integrity
- GenAI forgery detection using proprietary and third-party tools

- Rate-limiting, throttling, and abuse prevention on API endpoints
- Enterprise clients can opt into model isolation to further reduce data poisoning risk

Internally:

- Segregation of duties in finance, procurement, and data access
- Background checks during recruitment for sensitive roles
- Strict role-based access control (RBAC) and audit logs on all data and systems
- Financial approvals with dual sign-off thresholds
- Mandatory training on fraud awareness for employees in product, client-facing, and finance roles

---

5. Detection & Investigation

1. Platform-Detected Fraud

- All submitted documents are automatically scanned using AI and rule-based systems
- Fraud scores and indicators are presented to clients for review
- High-confidence frauds are flagged for client escalation
- Missed frauds (false negatives) can be reported by clients and are reviewed within 1 business day

2. Internal or External Allegations

- Any employee, client, or third party may report suspected fraud to:
  reportfraud@fraudfinder.ai (confidential inbox, monitored by the DPO and CEO)
- All reports are triaged and investigated discreetly by the **Fraud Operations Lead** or designated executive
- Cases may be escalated to legal counsel, regulators, or law enforcement as needed

---

6. Responses & Disciplinary Action

For External Parties:

- Confirmed fraud may result in:
    - Termination of services
    - Blacklisting of document fingerprints or IP addresses

    - Disclosure to affected clients or regulatory bodies
    - Legal action or criminal referral (in severe cases)

For Internal Staff:

- Employees found to have committed fraud face:
    - Immediate disciplinary action, up to and including dismissal
    - Notification to relevant regulators or professional bodies
    - Legal action for damages or recovery of funds

---

7. Reporting Obligations

We may be required to report certain fraud cases to:

- Financial Conduct Authority (FCA) or other regulators
- National Crime Agency (NCA), under the UK Proceeds of Crime Act 2002
- Clients' compliance teams under contractual agreements

We commit to full cooperation with investigations and will provide evidence packs where required.

---

8. Awareness & Training

- All employees receive **fraud awareness training** annually
- AI, product, and sales teams receive additional training on GenAI misuse and fraud vectors
- Clients are provided with best-practice guidance for fraud review workflows and risk controls

---

9. Review

This policy is reviewed **annually** or after a material fraud event. All changes require CEO approval.

Approved by:
Alexander Siedes, Chief Executive Officer

Effective Date: 06 July, 2025
Next Review Date: 05 January, 2026