fieldfisher

Using AI in Civil Fraud Investigations

02 February 2026

Fraud is one of the most common forms of crime in the UK. In 2024, it accounted for approximately 40% of all reported offences[1], with more than 3.3 million reports lodged, and confirmed losses of £1.17 billion[2].

Victims of fraud can issue civil proceedings to recover their losses provided they have clear, cogent and persuasive evidence to support their allegations. The standard of proof is the balance of probabilities (which is lower than in criminal cases, **beyond reasonable doubt**). Allegations of dishonesty are treated seriously, and evidential shortcuts are not tolerated.

The practical difficulty in fraud claims is scale. Modern fraud rarely turns on a handful of documents. Instead, it leaves behind vast quantities of digital material, including emails, messaging platforms, financial records, cloud storage, transaction data, internal records, and third-party data. Investigating involves analysing large datasets; this is where AI has become a valuable investigative tool.

Used properly, AI-assistance enables legal teams to sift through large datasets quickly, often at an early stage when there is a real risk of assets being moved out of reach. It can surface patterns, anomalies and connections that are difficult to detect through manual, batch-based review, allowing human reviewers to focus their time on analysis, judgement and case strategy. By contrast, delay or unfocused review can dilute the effectiveness of an investigation and weaken both recovery prospects and the overall litigation approach.

The role of AI in fraud investigations

In civil fraud matters, AI is most effective when used as part of a structured investigation and/or disclosure workflow, rather than as a standalone analysis tool. The objective is to identify and preserve evidence that supports urgent protective relief, narrows issues early, and strengthens recovery strategy.

In practice, AI is deployed after initial scoping and data hygiene steps, such as targeted collection, date and custodian filters, deduplication, email threading and initial keyword or concept testing. On these culled datasets, AI is then used to prioritise and organise material through a combination of technology assisted review and supervised Generative AI (GenAI) features embedded within review platforms, enabling lawyers to reach reliable conclusions more quickly, supported by an explainable audit trail.

What AI does well in a fraud context

The value of AI is not that it "finds the answer" but rather that it can help find reliable evidence more quickly. Decision-making is not delegated to the technology; AI acts as a practical aid, helping legal teams identify relevant evidence and reach safe, defensible conclusions earlier.

[1] According to the Crime Survey and National Crime Agency estimates, fraud accounted for around 41% of crime in English and Wales: https://www.nationalcrimeagency.gov.uk/threats-2025/nsa-fraud-2025

[2] https://fintechmagazine.com/articles/uk-finance-fraud-losses-flat-at-1-17bn-as-criminals-shift

In a well-governed workflow, AI tools can materially accelerate the tasks that most often drive cost and delay in fraud investigations. AI tools also assist lawyers in presenting evidence more clearly to the court. Some useful examples of AI assistance in fraud investigations include:

- → **Prioritising likely relevant material at speed:** Technology Assisted Review (TAR) ranks documents by likely relevance based on lawyer input, enabling earlier focus on core allegations in data-heavy cases.
- → **Surfacing patterns, anomalies and linkages:** Advanced analytics are often used to identify and highlight unusual transaction behaviour, inconsistent narratives, communication patterns or sentiment analysis that may otherwise be difficult to spot through batch-based review.
- → **Mapping relationships and activity:** Network and entity analysis assist in identifying patterns that connect people, entities, accounts and assets, particularly where there are layered corporate structures or cross border elements.
- → **Supporting faster, clearer decision making through GenAI assisted analysis:** Modern electronic disclosure / electronic discovery review platforms incorporate supervised GenAI features such as document summarisation, issue clustering and timeline construction, helping lawyers gain a broad understanding of large document-sets quickly. That said, it is essential that these GenAI outputs are verified by the lawyers who have conduct of the AI tool(s). Note (as expressed in the UK *Ayinde* judgment), decision making around the evidence remains with the lawyers using GenAI / AI tools, as well as supervising lawyer(s) (if any) to whom those lawyers report.

Supporting urgent court applications

Fraud cases often require urgent steps, including freezing orders, proprietary injunctions, search orders, delivery up and other interim relief designed to preserve assets and evidence.

Allegations of dishonesty require careful pleading and a properly supported evidential foundation. These applications succeed or fail on the quality of the evidence, its comprehensiveness and how clearly it is presented. AI can assist in assembling that foundation earlier and more efficiently, but professional judgement remains with the legal team. Examples of AI-assistance include:

- → **Identifying the core evidential documents earlier**, by accelerating review and enabling teams to move more quickly from suspicion to proof.
- → **Anchoring witness evidence and exhibits to that material**, ensuring statements and applications are grounded in specific, credible documents rather than inference.
- → **Providing earlier strategic clarity**, including what can safely be pleaded, what should be reserved, and where there may be evidential risks to avoid.

Investigative analytics and fraud risk signals

Organisations and public bodies increasingly use AI to identify fraud risk and prioritise investigations, with human investigators validating and acting on the outputs.

The UK Government has reported that the use of new technology and artificial intelligence in its counter fraud work, prevented or stopped over £480 million from being lost to fraud over a twelve-month period (April 2024 to April 2025). These results were linked to the deployment of new tools

fieldfisher

Toolkit and Practical Guidance for AI use in Fraud Investigations

Principle	What this means in practice	What clients should expect and ask
Transparency and explainability	AI assisted processes must be capable of explanation and defence if challenged. Teams should be able to show what tools were used, how they were configured, and how outputs were reviewed.	*Ask how AI is being used, what decisions it informs, and how the process would be explained to the court if required.*
Human oversight and accountability	Responsibility always remains with the lawyers. AI outputs must be reviewed, tested and verified. Sampling and quality control are essential, particularly in serious fraud matters.	*Expect active legal supervision. Ask how outputs are validated and what checks are in place to identify errors or bias.*
Compliance and defensibility	AI must enhance compliance with disclosure obligations, not shortcut them. Workflows should be documented, validated and aligned with court rules.	*Ask how the investigation and disclosure process is documented and how its defensibility is preserved if challenged later.*
Data security and confidentiality	Fraud data is often highly sensitive. Secure, approved platforms must be used, and confidential material should not be entered into public or consumer AI tools.	*Confirm where data is hosted, who can access it, and what security and contractual protections apply*
Proportionality and value	AI should reduce cost and complexity, not add unnecessary layers. The focus should be earlier insight and stronger evidence, not volume processing.	*Ask what the AI process is intended to achieve and how it supports faster, clearer outcomes.*
Auditability and traceability	Decisions informed by AI should be traceable through clear audit trails showing inclusion, exclusion and prioritisation decisions.	*Expect visibility at a high level into how key decisions were reached and how they can be evidenced if required.*

Key contacts

Fiona Campbell

Director, Dispute Resolution | Head of Technology, Innovation & Digital Evidence (TIDE)

+44 330 460 6620
fiona.campbell@fieldfisher.com

Alexandra Underwood

Partner, Dispute Resolution

+44 330 460 6584
alexandra.underwood@fieldfisher.com