FORUM OF INSURANCE LAWYERS

Informing Progress - Shaping the Future

FOIL Update 24th October 2025

The Increase in Fraud and the Response of UK Insurers

Fraudulent insurance claims are on the rise in the UK, which is imposing significant costs on insurers, policyholders, and public services. The Association of British Insurers (ABI) reported that the total value of detected fraudulent insurance claims in the UK was over £1.2 billion in 2024. Over 40% of these claims were related to motor claims, which showed an increase of 8% from the previous year.

Data from the National Crime Agency (NCA) suggests fraud accounts for 41% of all crime in the UK, making it the most prevalent crime against individuals. In addition to causing devastating impacts to victims, fraud results in severe harm to society and the broader economy by funding serious organised crime organisations in the UK and beyond. Improvements in technology, the level of punishment and the use of English have all contributed to the UK becoming a global magnet for fraud compared with other jurisdictions.

Scammers are adopting increasingly sophisticated techniques, including ghost broking, staged accidents, AI-assisted image distortion, and synthetic identities. Addressing fraud remains a strategic priority across the industry and, as such, insurers are increasing their investment in detection, collaboration, and prevention in response.

The Economic Crime and Corporate Transparency Act (ECCTA), in particular, the new corporate offence of "*failure to prevent fraud*", which came into effect on 1 September 2025,

increases the legal incentives on insurers and intermediaries to embed effective anti-fraud measures and has the potential to materially alter industry practice.

An Upward Trend

Independent fraud monitoring and industry bodies report a steady rise in recorded fraud; Cifas, which operates the UK's National Fraud Database, recorded a historic increase in fraud in 2024, with significantly more cases submitted than in previous years. This suggests evidence of growing criminal activity, but also of improved reporting.

Additionally, established insurance industry sources show that tens of thousands of dishonest insurance claims are identified each year, with the ABI estimating these totalled 72,600 in 2022, a figure that increased to 84,400 in 2023. These figures underline that insurance fraud remains a large-scale and persistent problem.

Insurers' own disclosures reinforce this point, with large providers reporting thousands of attempted frauds a year and the prevention of multi-million-pound losses. Aviva, for example, reported detecting more than 6,000 attempted frauds in the first six months of 2025 alone, preventing losses of more than £60 million and leading to several successful prosecutions. This equates to £344,000 in losses prevented every day, demonstrating the frequency of attempts and the financial stakes for insurers.

New Methods and Vulnerabilities

The nature of fraud is also changing as fraudsters exploit digital channels, social media and AI to fabricate evidence, edit photographs and create convincing false documents. Reports of manipulated vehicle images showing fake damage and other 'shallowfake' evidence have increased, promoting inflated or spurious motor and property claims.

Rapid developments in AI have also simplified the process of creating false identities, enabling criminals to make greater use of identity fraud, automated account takeover techniques, and organised networks that can exploit multiple insurers simultaneously. These developments make effective detection more complex and heighten the risk of fraudulent payments.

Industry Response

Insurers have responded by increasing their investment in anti-fraud capabilities, spending upwards of £200 million each year on detection and prevention methods, encompassing tools such as forensic analytics, specialist investigations teams, legal recoveries, and partnerships with law enforcement.

An integral part of modern anti-fraud efforts is the Insurance Fraud Bureau (IFB), which acts as an industry data hub by consolidating intelligence, running network-detection tools and supporting investigations that span multiple insurers and jurisdictions. In 2024–25, the IFB and its members championed advanced analytics and 'network' approaches that can identify

related claims across different companies, which has been a vital counter to organised fraud rings.

Technological tools now in regular use include machine learning models that flag anomalous claims, natural language processing capable of scanning large document sets, image forensics which detect manipulated photos, and cross-industry data matching that can identify suspicious patterns.

Furthermore, insurers are deploying predictive models to assign risk scores to claims and to prioritise cases for further human investigation. Large firms are building internal centres of excellence and appointing dedicated fraud prevention leads, while smaller firms increasingly outsource to specialist vendors or participate in shared intelligence services as a means of protection.

Collaboration remains a key component of effective, proactive prevention, with industry bodies, law enforcement, and fraud prevention services such as Cifas and the IFB sharing intelligence and operating referral routes. The result is improved detection rates and, where appropriate, improved criminal enforcement, with recent reporting noting a rise in successful prosecutions and custodial sentences linked to insurance fraud investigations.

Prevention Challenges

Despite the progress being made, clear obstacles persist. Robust data-sharing between firms holds legal and practical complexities, such as compliance with UK GDPR and data-protection obligations, which require careful contractual and technical controls. Insurers must therefore balance the need to detect cross-party fraud with the risk of unlawfully processing personal data.

Investment needs are also substantial, as building and maintaining advanced analytics, training fraud investigators, and conducting forensic work are expensive activities that smaller firms may struggle to resource. Additionally, automated detection will inevitably produce false positives, making a proportionate human oversight framework imperative to avoid injustice to honest policyholders.

A further and growing concern centres on the technologies used to combat fraud being turned to the advantage of criminals. Industry commentators have warned about AI being misused to fabricate convincing evidence and streamline deception, causing insurers to redouble efforts on provenance checks, metadata analysis, and multi-factor verification as ways to counter these threats.

Raised Expectations through the ECCTA

The new offence of failing to prevent fraud, recently introduced through the Economic Crime and Corporate Transparency Act (ECCTA), means an organisation can be held criminally liable if an associated person, such as an employee, agent or subsidiary, commits a fraud offence intended to benefit the organisation, and the organisation did not have reasonable fraud

prevention procedures in place. In addition, it is not necessary to show that company managers initiated or were aware of the fraud, or that the company did indeed benefit from such actions.

There is no one-size-fits-all approach to what is 'reasonable', but in most cases, it will involve implementing a range of measures and being able to prove that the organisation has taken active steps to engage with and enforce these measures. The test is likely to incorporate governance, risk assessment, staff training, monitoring, and rapid remediation measures. The effect is to push firms to move beyond ad-hoc activity toward documented, auditable, and proportionate anti-fraud frameworks.

For insurers and intermediaries, the ECCTA alters incentives in two important ways: it raises the legal stakes of insufficient controls, as boards must now consider the criminal consequences of systemic gaps, and it encourages more formalised record-keeping and independent assurance with the existence of clear procedures, evidence of regular testing and demonstrable efforts at prevention. These will be central to a firm's defence, and the Act will likely accelerate investment in prevention, governance, and inter-firm cooperation.

Practical Implications for the Insurance Sector

In practice, the ECCTA is expected to introduce a number of noticeable changes to firms' approach to fraud. Firstly, senior executives will be expected to participate in fraud-risk strategies. Firms will also expand training and controls across the distribution chain, including for brokers and third-party agents, to mitigate their risk exposure. Finally, insurers will seek greater assurance from outsourcing partners about their fraud prevention.

We should also see an increase in industry-wide initiatives that create shared, auditable standards for data-sharing, model validation, and information security. Regulators will also be watching, and failure to make demonstrable improvements could attract regulatory penalties as well as criminal consequences.

The insurance industry has responded to the rising and evolving threat of fraud with enhanced analytics, intelligence-sharing and enforcement development. Notable challenges remain, but the implementation of the ECCTA's new offence is a significant development. FOIL maintains in consultation with its members on this evolving topic, serving as a conduit for information sharing that will help reinforce the insurance industry's move from reactive detection to proactive prevention and support insurers in staying ahead of increasingly creative fraudsters.