TIME FOR A UNIFIED APPROACH IN CLAIMS MANAGEMENT

Fraud remains one of the biggest challenges facing the insurance industry. While technology and investigative techniques have advanced, the fight against fraud is still fragmented. To protect genuine customers, reduce loss ratios and safeguard industry reputation, anti-fraud measures must play a central role in claims management.

Today, fraud detection is inconsistent across insurers. This imbalance allows large numbers of fraudulent claims to go unnoticed, even though companies often handle similar portfolios. Automated fraud detection has helped to some extent, but without widespread adoption, its benefits are limited to those insurers with the necessary technology budgets.

The financial stakes are significant. In 2023, the ABI reported over £1.1 billion in fraudulent claims – a 4% increase from the previous year – with motor insurance accounting for nearly half a billion pounds. These costs are ultimately borne by honest customers through higher premiums and contribute to the sector's reputational challenges.

A key issue is the absence of minimum industry standards. Each insurer applies its own mix of technologies and investigative approaches, leaving the sector uneven. Some businesses are five to seven years behind their peers, yet all operate in the same market. This inconsistency creates vulnerabilities that fraudsters exploit, moving from one insurer to another in search of weaker controls.

The solution lies in collaboration. The industry must establish baseline standards for fraud prevention and detection, creating a common framework across insurers and supply chains. A harmonised approach would unlock new opportunities, including meaningful use of big data, enabling more effective identification and deterrence of fraudulent activity.

While technology is crucial, improvements can also come from smarter processes. Some insurers lack robust screening at underwriting, allowing known fraudsters to enter their books. Simple due diligence and better data sharing could prevent this. New fraud trends increasingly involve sophisticated fake documents, including AI-generated content, which require the right tools and training to identify and mitigate.

At Charles Taylor, we see fraud in everyday claims and complex, high-value losses alike. Fraud often begins opportunistically before evolving into repeat or professional behaviours wherever vulnerabilities exist. This is why a proactive, preventative strategy embedding fraud detection throughout the claims process is essential.

Insurance fraud is not a peripheral issue. It undermines customer trust, damages profitability and inflates premiums. The industry cannot afford fragmented approaches. A harmonised, collaborative strategy will protect insurers and restore confidence across the sector.

Bobby Gracey,
Head of Counter-Fraud, Charles Taylor

RECIPROCITY: THE ENGINE ROOM POWERING OUR COUNTER FRAUD CAPABILITY

Collaboration has long been our industry's superpower against insurance fraud. We've built the habit of sharing data and intelligence, joining the dots and coordinating collective action. We've shown that reciprocity works in practice and overcomes the otherwise limited visibility of any single insurer.

This culture did not appear overnight. Insurance has led the way in sharing data and intelligence. From the early days of claims sharing via CUE and MIAFTR, to pioneering fraud and device-data consortia. From adopting the National Intelligence Model to share intelligence safely and lawfully, to the operation of the IFB as the industry data and intelligence hub with its databases of proven and suspect fraud. Each step strengthened the same underlying principle: contribute and benefit.

Fraud keeps changing. So must we. And through 2025 we have seen a renewed emphasis on cooperation and reciprocity to ensure our collective capability keeps pace with evolving threats.

This is epitomised by the IFB's delivery of their Broadening the Membership programme, part of their strategy over the last three years. This modernised the membership structure to drive cross-industry reciprocity, enhanced member capability and extended IFB membership across product lines and the wider insurer ecosystem.

To me, three areas really stand out:

Modernised membership documents, placing reciprocity at the centre of collaboration and enabling the next level of data and intelligence sharing.

Simpler, yet still robust rules for members, improving protection of shared data while enabling timely use across the full membership.

A wider, connected membership base, strengthening overall sharing and the ecosystem's ability to support insurers.

With this programme delivered, the IFB's new five-year Connected to Protect strategy launched in October now goes further. It aims to broaden participation across products and partners, raise data quality and quantity, and deepen public and sector trust. The goal is not just bigger data. It is better outcomes: improved decisions, greater disruption, broader prevented losses, fewer victims.

For counter fraud leaders, the message is simple: reciprocate and cooperate. Keep contributing high-quality data, enable lawful and right-time use, and bring business partners onto the same page. This is how we will achieve the next step-change in collaboration.

Matt Gilham,
Director, Whitelk