SHUTTERSTOCK

Time for action

The UK's new Fraud Strategy must lean on civil process, private-sector muscle and operational boldness, argues **Frances Coulson**

The Government's *Fraud Strategy 2026–2029: Disrupting crime, supporting economic resilience and delivering justice* is an important statement of intent. Fraud is now the most prevalent crime affecting individuals and businesses in the UK. It is technologically enabled, borderless and increasingly industrialised. There are victims across the board – those defrauded of their money and often their self-respect, or worse, their life. Sometimes the people who commit fraud are victims because they are people who have been trafficked and forced to commit fraud on an industrial scale.

Fraud is only likely to get worse as fraudsters increasingly adopt artificial intelligence. Domestic and international law, action and regulation are not keeping up with the lawless, organised criminals who do not pause to consider, but simply do whatever it takes to get the greatest return without caring about collateral damage.

The Fraud Strategy acknowledges this reality, proposing a coordinated, system-wide answer to fraud built around disruption, safeguarding and response. This approach is supported by a new Online Crime Centre, a revamped national reporting service and the long promised Fraud Victims Charter.

All of that is welcome. But strategies do not stop fraudsters – action does. In my view, the success or failure of the Fraud Strategy will turn less on its architecture, and more on how boldly and practically it is implemented. Key themes include: elevating civil process to the same level of importance as criminal justice, fully mobilising the private sector as an operational partner, measuring success by outcomes that victims actually experience, and acting earlier, faster and at greater scale.

1. Civil process as a first response

The Fraud Strategy commits to delivering justice through both criminal and civil outcomes. That framing is overdue. Criminal prosecutions remain vital for punishment and deterrence, but they are rarely quick enough to stop dissipation of assets or to deliver meaningful, timely redress to victims. Even with significant investment in the near term, criminal courts and prisons will take time to catch up with fraud volumes, assuming the perpetrators actually reside within the jurisdiction. Confiscation orders can take years post-conviction and are fraught with difficulty. Why not prepare for, and seek, the confiscation order on conviction as part of the prosecution case (therefore using fewer state resources) and if not paid, bankrupt the perpetrator, let the trustee take the lot and distribute to victims, who are, of course, creditors?

By contrast, the civil courts already provide a powerful and well-tested toolkit: freezing orders, search and imaging orders, proprietary and tracing claims, third-party disclosure, receivership and insolvency processes, and more rapid cross-border enforcement. These remedies can be deployed within days, sometimes hours. Used properly, they can stop the money moving, expose the mule network and unlock data across banks, platforms and intermediaries long before a criminal case reaches charge. I recall a missing trader intra-community case some years ago where the criminal case took 10 weeks (some time after the civil case was concluded), whereas the civil trial took five days. Same facts, different audience and burden of proof.

Civil process can also deliver pragmatic justice. Interim recoveries, negotiated undertakings and civil settlements can also often return funds to victims sooner and at lower public cost. There is also a strong case for punitive damages and recycling a portion of successful recoveries into further disruption and enforcement, ensuring that fraudsters, rather than taxpayers, fund the fight against fraud.

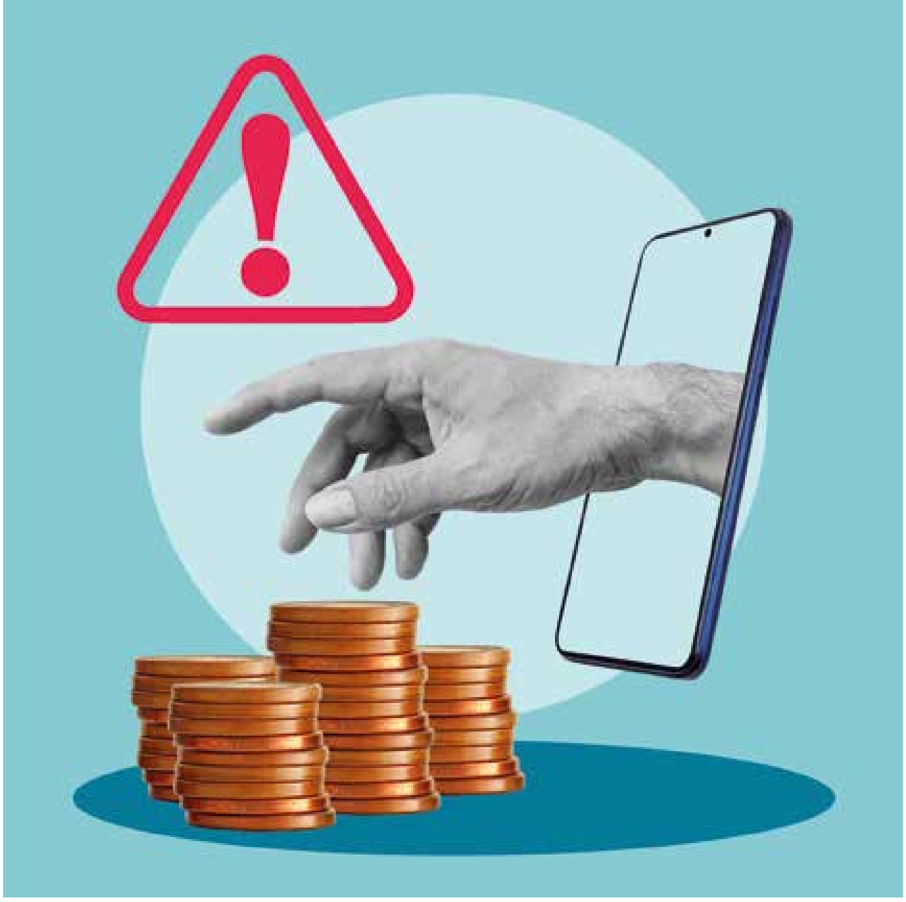
2. Harnessing private-sector muscle

The Fraud Strategy's proposal for an Online Crime Centre intends to bring together government, law enforcement, intelligence and private-sector participants in finance, telecoms and technology. There are other participants to consider, including private-sector office holders and creditors (victims). It is also important to get participation from the insolvency sector where both Companies House and the Insolvency Service play an increasingly efficient role. (The abuse of companies registration in England and Wales has been a fraudsters' gift, but now the Economic Crime and Corporate Transparency Act 2023 has given Companies House the power to stop that.) Designing the process to include private-sector muscle is crucial, because the levers that stop fraud at scale – bank account freezes, payment controls, SIM blocking, advert takedowns and platform moderation – sit largely outside the public sector.

> **Fraud is only likely to get worse as fraudsters increasingly adopt artificial intelligence**

If prevention is the goal, the private sector must be treated not as a stakeholder to be consulted, but as a co-designer and co-operator of disruption. That requires regulatory clarity and, where necessary, sensible relaxation to allow lawful, real-time sharing of signals and typologies without the paralysis brought about by the data-protection regime. It means a genuine 'no wrong door' model, where intelligence received by the Online Crime Centre is pushed simultaneously to banks, payment providers, telecoms networks and platforms, with clear and rapid service-level expectations.

It also means industrialising the response: shared analytics to identify ▶



mule herding (recruiting people to transfer stolen money) and high-velocity authorised push payment fraud, pre-agreed platform 'kill switches' for mass takedown of fraudulent content and standard cross-border templates – for example, for data requests – that allow international cooperations to function at the speed at which fraud now operates.

3. Putting victims at the centre

The proposed Fraud Victims Charter and the replacement of Action Fraud with 'Report Fraud' offer an opportunity to reset how the victim experience is judged. Too often, success is measured by inputs: referrals made, reports logged, prosecutions commenced. Victims experience success very differently.

For them, the questions are simple. Of course, they want the fraudster punished, but if the fraudster is a state actor or organised crime group, more interesting questions are: How quickly was the money frozen? How much was recovered? How long did reimbursement take? Was repeat victimisation prevented? A genuinely victim-centred model requires guaranteed triage within hours, not weeks, seamless handoffs between banks, platforms and the police, and clear, fair reimbursement pathways with independent recourse. It also requires communication (within limits so as not to prejudice an investigation). Too often, regulation (or the interpretation thereof) and timidity serve the fraudster, not the victim. Probably the biggest difference could be made immediately by empowering lower and middle operational management in the public sector, with ensuing hindsight audits for governance and for ongoing improvement of actions.

For corporate victims, particularly those affected by complex or organised fraud, the Fraud Strategy could normalise a civil criminal twin track: immediate private civil action running in parallel with law enforcement engagement, possibly with insolvency tools deployed early to preserve books, records and other evidence, compel disclosure and secure assets for distribution. That would save costs in the criminal process provided the audit trail and fairness are kept in mind. The Insolvency Service recently launched a civil enforcement regime consultation suggesting wider powers for the Service and office holders. It wants to make it easier for successful actions to be brought during formal insolvency so that money wrongfully paid to third parties prior to insolvency can be reclaimed and the impact of other transactions that are harmful to creditors can be reversed. This is to be welcomed so long as it is balanced with evidential fairness.

> **Too often, regulation (or the interpretation thereof) and timidity serve the fraudster, not the victim**

4. Operational boldness: earlier, faster, bigger

Fraud is now a data-driven industrial business. Counter-fraud responses must be equally industrial. The Fraud Strategy anticipates coordinated takedowns of infrastructure and cites high-impact operations as a model. The real test will be whether the system can intervene pre-harm and at platform scale.

Effective intervention will demand pre-emptive triggers – using risk signals to introduce payment pause before funds leave a victim's account (as happens with clearing banks now the risk is more at their door); genuine mass takedown capability supported by clear legal gateways; 24/7 operational capacity with access to urgent civil orders; and disciplined after action learning, so every disruption improves the next. There is no point in enquiries with action points that never see the light of day.

Societal outcomes

The *Fraud Strategy 2026–2029* correctly recognises fraud as a major threat to individuals, businesses and economic confidence. Its structural components are sound. The determinant of success will be operational pace, partnership and resolve. If civil process is normalised as a first response, private-sector infrastructure is embedded into the operational fabric, victim outcomes are treated as the primary metric, and the system acts boldly and early, the economics of fraud can be shifted decisively back in favour of the public. Then the UK might become an even nicer place to live.

Frances Coulson is a partner and head of insolvency and restructuring at Wedlake Bell. She is also co-chair of the R3 Fraud and Asset Recovery Group and president of INSOL Europe

SHUTTERSTOCK