



Bulletin

of The International Academy
of Financial Crime Litigators

ISSUE 6 | SPRING 2026

The UK Government's New Fraud Strategy: Key Implications for Enforcement and Compliance.



SUE THACKERAY

Introduction

In March 2026 the UK Government launched the [Fraud Strategy 2026-2029](#), which introduces a new landscape for tackling fraud. Fraud is now the largest type of crime in the UK, costing the economy an estimated £14.4 billion in 2023-2024. The Government recognises that fraud is a crime with significant consequences for both victims and the broader economy, and the new Fraud Strategy is a positive step towards tackling the problem. The core ideas are to improve data sharing, block more online crime at source, and create more resilient industry processes in vulnerable sectors.

In my view, it is a credible strategy that reflects a detailed understanding of the risks and the systems that contribute to fraud in the UK. It builds on the systems set out in legislation such as the Economic Crime and Corporate Transparency Act 2023, which introduced corporate criminal liability for failure to prevent fraud in England & Wales. Now it all comes down to the implementation. This article examines the strategy's key pillars and explores the practical implications for financial crime practitioners, including the increased dependence on civil remedies.

PROBLEMS WITH THE UK'S CURRENT APPROACH TO FRAUD

The Government's approach to fraud has historically suffered from a lack of information sharing between public bodies. This has meant that the fraud response has always been reactive and focused on the post-event investigation rather than targeting the underlying systems that enable fraud in the first place.

The Government has focused on criminal justice, but the system has not been able to achieve sufficient prosecutions to act as a real deterrent. The problem has only been getting worse, with the rise of tech-enabled fraud and AI-driven threats making it harder for the public to detect fraud. Fraud has become a low risk and profitable crime, which has allowed it to become so pervasive.

Financial crime lawyers have long argued that tackling fraud effectively requires a broader toolkit, including greater reliance on the private sector and the use of civil sanctions and enforcement mechanisms alongside traditional criminal justice approaches.

THE NEW APPROACH

The new fraud strategy focuses on three key strands: (i) disrupt (ii) safeguard and (iii) respond. The emphasis is clearly on the “disrupt” pillar, which represents a welcome departure from the traditional reactive model.

(i) Disrupt

The Government is notably shifting its approach to focus on disrupting the systems exploited by criminals to make fraud possible in the first place. It requires a proactive approach, acting early to deny criminals access to the systems they exploit and the profits of their crime.

The flagship announcement is the launch of a new Online Crime Centre. This is a £31 million public-private sector partnership intended to bring together various bodies including the Home Office, the NCA, the police, the intelligence community and private sector partners from the financial, telecoms, technology and cyber industries. It aims to share data and intelligence much more quickly and collaborate on interventions that can identify and intercept online fraud and cyber-crime at scale. The idea is to design technical solutions that support industry to put in place controls and processes early, reducing vulnerability and denying criminal access to the systems that they have historically exploited, and therefore the proceeds of their crime. The strategy also focusses on collaborating with the private sector to deliver interventions that address their vulnerability to fraud; in particular in telecoms, online and financial services. The attempt to address unauthorised fraud in the financial services sector is of particular interest. Since 2024, UK banks have been required to reimburse losses up to £85,000 for APP fraud (where victims are deceived into willingly transferring money). This was perhaps a missed opportunity, as this figure was reduced from the much more meaningful £415,000 due to lobbying from the banking sector, and has not incentivised the banks to take proactive steps to prevent the fraud in the first place. Whilst any reimbursement scheme is still useful, it is an example of the Government’s

focus on fixing the outcome of fraud, rather than disrupting the cause of the problem. The Fraud Strategy acknowledges this by launching a call for evidence to assess the scale, drivers and enablers of unauthorised fraud. The Financial Conduct Authority (FCA) also plans to share recommendations for preventing APP fraud with the financial services sector.

The imminent changes to the cryptoasset firm landscape are another positive systemwide development. A new regime comes into force in October 2027 which will mean that cryptoasset firms will need to be authorised by the FCA and to comply with its rules. Activities such as operating a cryptoasset trading platform in the UK will become regulated activities. This is a significant change that means that cryptoasset firms must obtain authorisation, maintain governance and risk management systems and implement robust anti-money laundering controls. The FCA expects firms to be able to monitor transactions and block transactions to high-risk wallet addresses. This degree of regulation should make it easier for victims of fraud to trace cryptoassets, a notoriously difficult area.

(ii) Safeguard

The “Safeguard” pillar focuses on protecting individuals and businesses by providing clearer guidance and more support for vulnerable groups. This should improve public and business resilience to fraud.

It includes the expansion of a national campaign called “Stop! Think Fraud”, to raise public awareness and resilience to fraud. It also focuses on support for high-risk sectors and engagement with the private sector on issues such as identity verification.

(iii) Respond

This pillar looks to improve on reporting, investigation and victim care. The City of London has just launched a new Fraud Report service, which replaces Action Fraud as our national platform for reporting cybercrime and fraud. We are supportive of the idea of a centralised fraud reporting system, but Action Fraud was clearly not fit for purpose. In practice, clients were reporting fraud to Action Fraud simply to obtain a reference number for insurance purposes, rather than with any expectation that Action Fraud would assist their case. We hope that Fraud Report can provide a faster response and better recovery outcomes. However, we would also like to see the Government make good use of the critical data that Fraud Report will collect (see further below).

WILL THE STRATEGY WORK?

There is a general consensus that the Fraud Strategy is a positive step in the right direction. However, the implementation will be key and there are some important factors that the Government must focus on.

1. Further investment

The Government is committing to investing over £250 million in fraud prevention and response measures by 2029. This is a welcome announcement and demonstrates that there is real political will to address the problem, but it still pales in comparison to the magnitude of the problem and the economic impact. The scale of the issue will necessitate further investment and commitment to tackle fraud beyond 2029 as well.

The Fraud Strategy references the need to future-proof against emerging technology, deepfakes, stablecoins, blockchain and new payment methods. The next wave of payment innovation and the fraud risks it creates will only offer fraudsters more opportunities to exploit the system. We therefore need to ensure that our response is dynamic, and able to adapt to a changing landscape. This will inevitably require further investment.

2. Successful implementation

One of the most positive aspects of the new strategy is the recognition that fraud is a systemic, industrialised issue. For example, fraudsters have been able to exploit loopholes by creating fake companies or impersonating businesses. A particular problem that we regularly see in practice is criminals intercepting legitimate emails and sending fake invoices. The Fraud Strategy introduces mandatory electronic invoicing for VAT invoices from April 2029, which is a positive initiative that should allow suppliers to generate and send invoices through secure digital systems. However, the Government must ensure that the implementation of this is successful through a well-resourced information campaign. The infrastructure must also be impenetrable, to avoid simply creating another system that fraudsters can exploit.

3. International outlook

The Fraud Strategy also correctly identifies that fraud is a cross-border problem that requires an international outlook. The Government says that

it will pursue more partnerships with high-priority countries, like it has done with Nigeria and Vietnam. Continuing to invest in global research and skills development will be critical to long-term resilience, as fraudsters often operate overseas and target the UK from jurisdictions that are outside of our regulatory framework.

4. Reliance on civil remedies

The Fraud Strategy states that the Home Office is supporting law enforcement pilots focused on pursuing legal action against criminals and recovering money for victims through civil law by 2028. It is also considering introducing civil penalties for fraud and facilitating money laundering as an alternative to the criminal law.

This follows, for example, the introduction of civil penalties in tax fraud by HMRC. The lower burden of proof required under the civil standard in England & Wales would also potentially help with some of the evidential challenges that characterise complex criminal fraud trials.

However, the Fraud Strategy does not contain any detail on what the proposals for civil recovery might look like, or how they would be resourced. Within public bodies, there is a lack of staff with capacity and ability to pursue civil remedies and they have understandably focused on criminal recovery. One of the problems with the traditional civil fraud remedies is that the amount of money that has been lost by an individual or a single business is often not sufficient to justify the expense of recovering it. This is particularly true where individuals or businesses have just been defrauded and may not have the resources to spend further money on a civil claim.

However, fraudsters often target multiple people with the same fraud. If victims were able to find each other, then they could form a collective group and litigate much more effectively. The Report Fraud database is a key repository of this information. The Government should consider the viability of a scheme whereby they (i) analyse the crimes being logged via Report Fraud and (ii) identify groups of victims of the same crime. The Government could then work with external law firms who specialise in financial crime (with criminal and civil expertise) to assess whether a group of victims could make a successful claim for recovery in the civil courts, which could also be funded by alternative fee arrangements or third party funders to reduce or

eliminate up front cost to the individual victims who might have lost their life savings to fraud. This proposal would clearly involve challenges, including in relation to volume and data-sharing, but is worth exploring as an additional tool in the response to fraud.

CONCLUSION

This Fraud Strategy has been long in the making, and its ambition is to be welcomed. The recognition that fraud is a systemic, industrialized problem represents a shift in the Government's thinking. The three-pillar framework of disrupt, safeguard and respond provides a coherent architecture for the strategy. However, the detail and implementation will be critical. The Government must ensure it focusses on the areas outlined above in particular if this strategy is to be a success. In addition, the international dimension cannot be overstated. A domestic strategy can only be effective if it is supported by international partnerships and it is vital that public bodies and lawyers continue to engage across borders to assess new risks as they develop.

For practitioners advising clients on fraud risk and recovery, there are several key priorities. Organizations must review their compliance frameworks in light of the failure to prevent fraud offence, ensuring that adequate procedures are in place and documented, as scrutiny will only increase because of this strategy. Secondly, firms operating in the financial services sector should engage closely with the new regulations, ensuring that they fully understand the requirements. Thirdly, practitioners advising victims of fraud should monitor the development of the civil recovery pilots. The potential for group litigation, potentially facilitated by data from the new Report Fraud platform, could represent a significant new avenue for recovery.

AUTHOR

[Sue Thackeray](#) is a partner at Kingsley Napley LLP in London. She is a highly experienced commercial litigator who is widely sought after for her strategic expertise in civil fraud and asset recovery cases, often where criminal proceedings co-exist.