


The Home Affairs Committee launched another inquiry into fraud - Stop! Think Fraud

20 February 2024  Paul Wainwright

Fraud is the most common crime in England and Wales. It amounts to 40% of all crime, but only received 2% of police resources last year. Despite this, according to the NCA nearly 86% of fraud instances are unreported. Fraud has truly reached epidemic proportions in the UK.

Corporate bodies are no doubt seeking to implement and adopt suitable strategies and policies to ensure they do not become victims and are not prosecuted for failing to prevent fraud as the Economic Crime and Corporate Transparency Act 2023 beds down following Royal Assent last year. But as most fraud is committed online what is being done to protect the public, and control and reduce the incidence of fraud?

Despite the earlier Home Office aims to “stop fraud at source” as set out in their [Fraud Strategy](#) launched in May 2023, the earlier National Fraud Initiative Report 2022, and an inquiry in 2022 which made over 60 recommendations, the latest inquiry announced in September 2023 seems to have been subsumed by another campaign seen as a “bold” “powerful tool” to prevent online fraud announced on 12 February 2024 called [Stop! Think Fraud](#).

This appears to be another catchy slogan, but some political commentators consider it “too little too late”. Will the campaign and the inquiry’s recommendations be another example of failing to grasp the fundamentals by kicking the fraud issue into the long grass or will the UK Government finally become serious about the action it needs to take and put some money into [fraud prevention and deterrence](#)?

Further, are the agreements with Tech Companies and the implementation of a National Fraud Squad (with 400 new investigators) going to make much difference? No doubt the recent images on the news of officers breaking down doors and making arrests will offer some solace. However, beyond the City of London Police, the SFO, and the DCPCU making arrests, prosecutions are few. In part, this may be due to the general squeeze in resources available within the criminal justice system. The value of deterrent messaging despite these inherent challenges should not be ignored.

The Home Affairs Committee have said they will examine the impact of fraud on victims and how they are supported in the aftermath. It further aims to assess the efforts being made to address fraud originating from abroad, along with assessing the effectiveness of the recent fraud strategy. The Committee will also look at how the growth of artificial intelligence and new technologies could transform the way in which companies tackle this form of crime.

This all needs some context of course and the [written evidence](#) to the Committee by stakeholders in academia, consumer groups, retail and finance sheds light on experiences of fraud across the economy, and how best this problem might be addressed.

It is clear that funding of policing and prosecutions and the criminal justice system needs to be addressed. Fewer than 1% of cases reported to Action Fraud result in a criminal justice outcome according to the House of Commons report published in 2023; and of the 27,000 cases referred to the Police less than 5% result in a charge or prosecution. The formation of the National Fraud Squad, and the City of London Police as the lead force does little to hide the complexity of the fraud landscape across the UK with 43 forces in England and Wales and Regional Organised Crime Units (ROCUs), the NCA, SFO, the NHS Counter-fraud Authority and the Public Sector Fraud Authority all offering different strategic approaches. There is a call for greater enhancement and co-ordination in the law enforcement structure, easier intelligence-sharing and a sustainable funding model.

For corporate entities (including public bodies) there has been a plea in some academic quarters for significant reform to “fraud reporting” - for it to be made mandatory and placed on a similar footing to AML or Terrorist Financing with a failure to disclose being classed as an offence in its own right by amending the Fraud Act 2006. This burden will likely fall on public bodies as well as the banks and financial institutions but could potentially be offset by the impact of the Economic Crime Levy or similar penalties from FCA financial-crime-related prosecutions. At a higher level the ability to obtain and exchange information by the submission of SARs would no doubt add valuable financial intelligence to law-enforcement capability and go in part to stopping organised fraud at source. It does not however appear to be under active consideration at this time.

A key issue in implementing any strategy is recognising that fraud is perpetrated against individuals, business and the state, with varying degrees of sophistication and volumes, from opportunist exploits to larger scale organised criminal activity. Add into the mix the increasing use of technology, in AI generated text scams, deep fake videos, and voice cloning and the interventions effective to put a halt to the escalating number of fraud events is quite a challenge. AI in fraud defence is one option but it is still in its infancy, and human based counter-fraud strategies will still remain the predominant and effective method of identifying and deterring fraud.

Avoiding victimisation also comes from education, awareness and support. Supporting and protecting whistle blowers is paramount to raising this issue and an area which needs significant reform but is regrettably absent from the Government’s current policy initiatives. It remains the case that victims of fraud are often the most vulnerable in society. They are coerced, gaslighted and emotionally manipulated into parting with their money. Academic research shows this leads to a stigma and shame leading to reluctance to reporting or even talking about the issue giving the perpetrators a significant advantage. Tackling fraud according to Trading Standards Scams Team should start with reframing the issue of vulnerability and recognising that fraud has a financial and emotional impact on all victims be they individuals or organisations. Signposting of such support – be it the right channel to report, remains vague and more needs to be done to support and protect victims. It is recommended that building a suitable national framework to educate and regularly raise public awareness will direct public outrage to the perpetrator and avoid negative victim blaming.

UK Finance has rightly pointed to the international dimension to fraud with funds transferred to other jurisdictions and the need for Payment Service Providers to engage with recipients to freeze accounts and where possible repatriate funds. Legislative barriers across jurisdictions prevent meaningful collaboration – both in terms of data sharing and accessing funds, but other countries such as Brazil and the Netherlands have adopted technology and active transaction monitoring to flag and stop fraudulent transactions. If fraud were placed on Financial Action Task Force’s (the global money laundering and terrorism organisation) agenda for instance it may significantly enhance national standards to seek out and disrupt serious organised financial crime and cyber fraud. Which? advocates a fairer more effective reimbursement model for victims beyond the Payment Services Regulators Contingent Reimbursement Model (CRM) Code to include international jurisdictions in light of the significant volume of Authorised Push Payment fraud committed online. This remains very much on the wish-list and not an immediate priority for legislators at this time.

Despite the inquiry filling Parliamentary time with further well-rehearsed narratives around solving the fraud problem, there seems to be a genuine cross-party desire to raise awareness and tackle this serious issue. It is significant that there is clear engagement from all sectors of the economy given the estimated £190bn lost to the UK economy each year.

It remains an all-pervasive problem and a significant societal issue which touches on all aspects of our daily lives. The changes in the legislative and regulatory landscape under the Online Safety Bill and the Economic Crime and Corporate Transparency Act 2023 should help but may not go far enough to stop the volume of fraud and its increasing sophistication.

Key contact



Paul Wainwright

Partner

paul.wainwright@brownejacobson.com

+44 (0)121 237 4577

Related expertise

Services

| | | |
|-----------------------------|------------------------------------|----------------------------------|
| Business crime and fraud | Criminal compliance and regulatory | Fraud and asset recovery |
| Counter fraud for insurance | | International trade and commerce |