‘To exchange or not to exchange, that is the question? A critical analysis of the use of financial intelligence and data sharing to tackle fraud’

Professor Nic Ryder
Cardiff University
Thursday 8th May 2025
12.05pm
ICA Future of FinCrime & Compliance - Summit
rydern@cardiff.ac.uk

Abstract

- The presentation is divided into five parts:
  - Part I – identifies the extent of fraud, outlines its threat and recent policy developments.
  - Part II – identifies the fraud reporting mechanisms
  - Part III – uses case studies to appraise the counter-fraud reporting mechanisms
    - Action Fraud
    - The Police
    - Social Media
    - Telecommunications
    - Tax Fraud
    - Terrorist Financing
  - Part IV – highlights data sharing mechanisms
  - Part V – provides a summary of the conclusions and recommendations

Part I – The extent

- Fraud is the most prevalent crime in the United Kingdom, accounting for over 40% of reported crime (ONS, 2023)
- Conservative estimates suggest that the annual UK fraud losses total £219bn (Crowe et al, 2023)
- The Crime Survey for England and Wales (CSEW) year ending (YE) December 2024 estimated 4.1 million fraud incidents. This was a 33% increase, compared with the YE December 2023 survey (ONS, 2025)
- 86% of fraud is not reported (NCA, n/d)
- 70% of fraud originates overseas (HM Government, 2024)
- The precise scale of fraud in the UK is unknown and remains an **intelligence gap.**

Part I – the threats

- Fraud presents a significant threat to:
  - UK economy (HM Government, 2023; NRA, 2020)
    - Approximately 18% of companies have been a victim of fraud (Stop Scams UK, 2024)
  - National security (Wood *et al*, 2021, Ryder 2024)
  - Serious Organised Crime (Levi, 2014, Winchester 2020, Perry and Brody, 2011)
  - Companies (NCA, n/d)
  - Citizens (HM Government, 2023)
  - Also see Home Office (2024)

Part I – Policy Developments

- Economic Crime Plan 1 (2019-2022)
- The Beating Crime Plan (2021)
- Economic Crime Plan 2 (2023-2026)
- Fraud Strategy (2023)
- The extension of failure to failure to prevent model to fraud Economic Crime and Corporate Transparency Act (2023)
- Fraud has been added to the Strategic Policing Requirement (2023)
- Economic Crime and Corporate Transparency Act (2023) data sharing provisions (section 198)
- Home Affairs Select Committee (2024)
- Reimbursement (2024)
- New Fraud Strategy expected end of 2025 (2025)

Part II – Fraud Reporting Systems

- Action Fraud
- HM Revenue Customs
- Department for Work and Pensions
- Home Office
- Serious Fraud Office
- Financial Conduct Authority
- Trading Standards
- Cifas
- UK Finance
- Financial Institutions
- National Crime Agency
- The Police
- Telecommunications Sector
- Social Media Companies
- Age Concern

Part III – Case Studies

Action Fraud

- Victim dissatisfaction (House of Commons Committee of Public Accounts, 2023)
- Limited public awareness (Smith et al, 2024)
- Absence of investigative powers
- Low success rate
- Limited resources
- Technical weaknesses
- Focus on compensation deterring reporting

The Police

- Fraud is not a priority (Police Foundation, 2023; HMICFRS 2019)
- The inadequacy of existing resources (Fraud Advisory Panel, 2023)
- 1-2% of police resources allocated to fraud (House of Commons Justice Committee, 2022; Home Office, 2023)
- Police forces adopt different approaches (NAO, 2017)
- 1,000 specialist police officers across 43 police forces (House of Commons Justice Committee, 2022)

Part III – Case Studies

Social Media

- Fraudulent content rife on the internet (Which?, 2022)
- Majority of fraud originates on the internet (UK Finance, 2022)
- Meta accounted for 87% of all investment fraud cases reported to TSB (Home Affairs Select Committee, 2023)
- Online Safety Act 2023 (no fraud reporting requirement)
- Online Fraud Charter
- Social Media not bound by the AML/CTF reporting obligations

Telecommunications

- 75% of UK population has received a suspicious message, in the form of either a text, recorded message or live voice call to a landline or mobile
- 40.8 million adults in the UK (Home Affairs Select Committee, 2023)
- Telecommunications Security Act 2001
- Communications Act 2003
- Telecommunications Charter (2021)

Part III – Case Studies

Tax Fraud

- HSBC Private Bank (Suisse) assisted wealthy clients to evade paying tax
- International clients' details would not be disclosed
- HMRC claimed it was not responsible for investigating money laundering and was prohibited from sharing information
- Activities of Suisse were revealed to the FCA and other LEAs in 2015, following the leaks to the media.
- Five years for FCA to become aware of allegations of criminality

Terrorist Financing

- Terrorist financing fraud typology (Ryder, 2024)
- Plethora of data sharing mechanisms (Ryder, 2024)
- Disconnected fraud and terrorist strategies
- Home Affairs Select Committee (2024)
- London Tube Bombing (July 7, 2005)
- Manchester Arena Bombing (May 22, 2017)
- London Borough Market (June 3, 2017)

Part IV – Data Sharing

- Law Enforcement Agencies and other Public Authorities:
  - Legal Gateways
  - Information Sharing in Practice
- The Sharing of Data between the Private Sector and LEAs:
  - The obligation to report suspected fraud by the private sector to LEAs is not straightforward
  - Criminal Finances Act 2017
  - General Data Protection Regulation and the Data Protection Act 2018
- Sharing of data in the Public and Private Sectors
  - Public Sector
    - Serious Crime Act 2007
    - Digital Economy Act 2017
    - Counter Fraud Data Alliance
    - National Fraud Initiative
  - Private Sector
    - Proceeds of Crime Act 2002
    - Crime and Courts Act 2013
    - Criminal Finances Act 2017
    - Economic Crime and Corporate Transparency Act 2023

Part V – Conclusions/Recommendations

Conclusions

- Fraud poses a significant threat (terrorism and organised crime)
- Too many reporting mechanisms – intelligence gap
- Current system is not fit for purpose
- Piecemeal strategy – kicking fraud into the long grass
- Lack of political will to replace Action Fraud
- Lack of resources
- Case studies highlight a loopholes and a reluctance to share data
- The benefits of data sharing are not yet fully developed and are immature

Recommendations

- Change of policy needed
- The legal gateways reformed to compel, rather than simply permit data sharing
- Increased funding:
  - Economic Crime Levy
  - Cross-governmental Economic Crime Fighting Fund
  - Reallocation of financial penalties from the FCA
- Automatic exchange of information
- Reform UKFIU