'To exchange or not to exchange – that is the question. A critical analysis of the use of financial intelligence and the exchange of information in the United Kingdom'

Professor Nicholas Ryder and Dr Samantha Bourton[1]

[1] Professor Nic Ryder (School of Law and Politics, Cardiff University) and Dr Sam Bourton (Bristol Law School, University of the West of England, Bristol).

Abstract

This article examines the international standards relating to information exchange, identifying its importance in relation to combatting financial crime. The paper critiques the results of the Financial Action Task Force's Fourth United Kingdom Mutual Evaluation Report, focusing on its conclusions in relation to the exchange of information between Law Enforcement Agencies. The second section provides two case studies, which serve to highlight flaws in the UK's legal framework.

Introduction

The most important mechanism to address the threat presented by financial crime is the use of financial intelligence, often gained from the submission of suspicious activity reports (SARs) to the financial intelligence unit (FIU), and subsequent exchange of information between competent authorities. The international anti-money laundering (AML) and counter-terrorism financing (CTF) legislative provisions from the United Nations (UN) and European Union (EU) are supported by the Recommendations of the Financial Action Task Force (FATF), which was established in 1989,[2] and is the 'world standard setter in the fight against money laundering'.[3] The FATF promotes 'measures for combating money laundering, terrorist financing and other threats', through its Recommendations.[4] Members of the FATF, such as the United Kingdom (UK), are subject to a peer-review process, with Mutual Evaluation Reports (MERs) recording the level of compliance.[5] In its 2018 MER of the UK's compliance with its Recommendations,[6] the FATF rated the UK's AML/CTF regime as the best in world.[7] One of the FATF's key findings was that 'co-operation and co-ordination between agencies on AML/CFT issues is a strength of the UK system'.[8] Therefore, the UK was rated as in full compliance with Recommendations 2, 30 and 31, which require national coordination and cooperation, including the exchange of information, between Law Enforcement Authorities

[2] G7, 'Economic Declaration' (16 July 1989) <http://www.g8.utoronto.ca/summit/1989paris/communique/index.html> accessed May 10 2022.
[3] A Damais, 'The Financial Action Task Force', in WH Muller, CH Kälin, JG Goldsworth (*Eds*), *Anti-Money Laundering: International Law and Practice* (John Wiley & Sons 2007) p.71.
[4] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations* (Financial Action Task Force 2012).
[5] The MERs are conducted using FATF, 'Methodology For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CTF Systems' (Updated October 2021) <www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf> accessed May 10 2022.
[6] Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report* (Financial Action Task Force 2018).
[7] ibid at p.5. Also, see HM Government 'UK Takes Top Spot in Fight Against Dirty Money' (December 8 2018) <https://www.gov.uk/government/news/uk-takes-top-spot-in-fight-against-dirty-money> accessed March 4 2023.
[8] ibid at p.37.

(LEAs).[9] The UK was also considered to have moderate to high levels of effectiveness to Immediate Outcomes 1 and 6, concerning risk, policy and coordination, and financial intelligence, as well as Immediate Outcomes 7 and 9, concerning effective money laundering and terrorist financing investigations. However, this paper questions these findings by presenting case studies that will serve to demonstrate inherent flaws in the UK's ability to ensure the exchange of information between LEAs to detect and address financial crimes. This is a significant weakness in the UK's AML/CTF framework, for the FATF, the European Union (EU) and others, have all stressed the importance of national LEA coordination and cooperation.

Despite the importance of information exchange for the purposes of investigating financial crimes, very little has been written about this topic. The financial intelligence gathering provisions have been the subject of academic criticism,[10] and several studies have explored the laws and methods used to obtain financial intelligence for the purposes of combatting fraud.[11] However, few studies focus on the exchange of information collected on a national level. The existing literature on information exchange tends to concentrate on inter-EU cooperation between security agencies, LEAs, and Financial Intelligence Units (FIUs) for the purposes of detecting money laundering and terrorism.[12] There is also a growing body of literature

[9] Financial Action Task Force (n 4).
[10] N Ryder, 'Cryptoassets, Social Media Platforms and Defence against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown' (2020) 8 Journal of Business Law 668; S Kebbell, 'Everybody's Looking at Nothing - The Legal Profession and the Disproportionate Burden of the Proceeds of Crime Act 2002' (2017) 10 Crim LR 741 and Law Commission, *Anti-Money Laundering: The SARs Regime Report* (Law Com No 384, 2019).
[11] L Pasculli, 'Coronavirus and Fraud in the UK: From the Responsibilisation of the Civil Society to the Deresponsibilisation of the State' (2020) 25(2) Coventry Law Journal 3; MJ Betts, *Investigation of Fraud and Economic Crime* (OUP 2017) and A Doig, *Fraud: The Counter Fraud Practitioner's Handbook* (Gower 2012).
[12] M Kaiafa-Gbandi 'Information Exchange for the Purpose of Crime Control: the EU Paradigm for Controlling Terrorism – Challenges of an "Open" System for Collecting and Exchanging Personal Data' (2019) 9(2) European Criminal Law Review 141; S Lule 'International Cooperation Combating Financial Proceeds of Crime' (2021) 7(1) European Journal of Economics and Business Studies 37; G Pavlidis 'Financial Information in the Context of Anti-Money Laundering: Broadening the Access of Law Enforcement and Facilitating Information Exchanges' (2020) 23(2) JMLC 369; M Den Boer 'Counter-Terrorism, Security and Intelligence in

concerning the international exchange of information in tax matters for the purposes of combatting offshore tax evasion,[13] as well as the implications of such exchanges on the right to privacy.[14] Nevertheless, there are no national evaluations of the legal powers and gateways used to obtain and exchange information between LEAs in the UK, which are tasked with investigating terrorism, money laundering, fraud, and tax evasion. This oversight has led to an uncritical acceptance of the appropriateness of the UK's legal and practical mechanisms for obtaining and exchanging information between LEAs for the purposes of preventing, detecting and combatting financial crimes, as evidenced by the FATF MER. This paper challenges conventional wisdom through two case studies, which demonstrate that national coordination in financial crime investigations is urgently in need of improvement. Additionally, this paper serves to rectify the omission in existing literature by providing a unique examination of the UK's legal framework pertaining to information exchange in terrorist financing and tax evasion investigations. By providing a holistic examination, this paper reveals previously undiscovered inadequacies in the existing framework and makes timely recommendations for reform.

The paper begins by identifying the international standards relating to information exchange, identifying its importance in relation to combatting terrorist financing and tax evasion, by drawing on studies from the FATF, the Organisation for Economic Co-operation and Development (OECD) and the EU. This section critiques the results of the UK's Fourth MER, focusing on its conclusions in relation to the exchange of information between LEAs. The second section provides two case studies which serve to illustrate the importance of information

the EU: Governance Challenges for Collection, Exchange and Analysis' (2015) 30(2-3) Intelligence and National Security 402.

[13] N Noked 'Tax Evasion and Incomplete Tax Transparency' (2018) 7 Laws 31; X Oberson, *International Exchange of Information in Tax Matters: Towards Global Transparency* (Edward Elgar 2015); DS Kerzner and DW Chodikoff, *International Tax Evasion in the Global Information Age* (Palgrave Macmillan 2016).

[14] E Virgo, 'Trust Registers and Transparency: A Step Too Far?' (2019) 33(3) Tru LI 95; A Haynes, 'Corporate Privacy or Public Nakedness?' (2018) 39(7) Comp Law 209 and F Noseda, 'Common Reporting Standard and EU Beneficial Ownership Registers: Inadequate Protection of Privacy and Data Protection' (2017) 23 T&T 404.

exchange and highlight flaws in the UK's legal framework that enable LEAs to obtain and exchange information. Following this comprehensive analysis, the final part also provides recommendations for reform. In particular, the paper recommends within the case studies that the reporting of suspected fraud should be mandatory, placing it on a similar statutory basis as money laundering and terrorism financing. Furthermore, the paper proposes a series of legislative amendments to the Commissioner for Revenue and Customs Act 2005 (CRCA) that would require employees of His Majesty's Revenue & Customs (HMRC) to exchange information where there is suspicion of money laundering or terrorism and would provide HMRC with a statutory crime prevention function.

Part I – International Standards on Information Exchange

One of the most important mechanisms to address financial crime is the use of financial intelligence and the related exchange of information. In order to facilitate the exchange of information between reporting entities, FIUs and LEAs, the international AML/CTF and tax evasion provisions, including the FATF Recommendations and the OECD Principles, provide a template for nation states to follow. This part of the paper provides a detailed overview of the international standards, which are later used as a benchmark, to determine the UK's level of compliance.

The Financial Action Task Force

Money laundering and terrorist financing demand a global co-ordinated response. The international AML framework originated in the United Nations (UN) Vienna, Palermo and

Corruption Conventions,[15] whilst the CTF framework can be found in the International Convention for the Suppression of Terrorism Financing and several UN Security Council Resolutions following the terrorist attacks in 2001.[16] The AML/CTF framework has been further developed by the FATF, which issued Recommendations providing its members with a template of AML/CTF legal measures.[17] Each version of the Recommendations has been implemented in the EU through a series of Directives.[18] The Recommendations mean that countries, irrespective of their economic size, are subjected to the same standards.[19] The Recommendations require countries to criminalise money laundering and terrorist financing, as well as adopt measures to enable the confiscation of the proceeds of crime.[20] Of relevance here, is the gathering and exchange of financial intelligence through Recommendations requiring the identification of those who enter into transactions,[21] including those who operate through legal entities and other arrangements,[22] as well as the submission of SARs to the FIU.[23] The Recommendations also provide for cooperation at both the international and domestic level. At the international level, the Recommendations require states to provide international

[15] Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (adopted 20 December 1988, entered into force 11 November 1990) 1582 UNTS 95 (Vienna Convention); Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 29 September 2003) 2225 UNTS 209 (Palermo Convention) and United Nations Convention against Transnational Organized Crime (adopted 15 November 2000, entered into force 29 September 2003) 2225 UNTS 209.
[16] See for example, S.C. Res, 1373, U.N. SCOR, 56th Sess., 4385th Mtg.
[17] Financial Action Task Force (n 4).
[18] See most recently, Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on Combating Money Laundering by Criminal Law [2018] OJ L 284/22; Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU [2018] OJ L 156/43.
[19] If a country does not comply with the Recommendations, it could be placed on the grey list, which was previously referred to as the non-co-operative countries and territories list. See M Riccardi, *Money Laundering Blacklists* (Routledge 2022).
[20] ibid, Recommendations 3 and 5 (criminalisation) and 4 (confiscation). Recommendations 6 and 7 concern the implementation of targeted financial sanctions.
[21] ibid, Recommendation 10 and 11, Recommendation 22. Enhanced measures must be taken when dealing with specific customers or risks, such as politically exposed persons, Recommendation 12, correspondent banking relationships, Recommendation 13, and persons or transactions with higher risk countries, Recommendations 19 and 23.
[22] ibid, Recommendations 24 and 25.
[23] Recommendation 20 and 21, Recommendation 23. A FIU should be set up to receive and analyse SARs, Recommendation 29.

cooperation, including mutual legal assistance and extradition for related criminal offences.[24] At the domestic level, the FIU, LEAs and supervisors must 'have effective mechanisms in place which enable them to cooperate … coordinate and exchange information … with each other concerning … [preventing] money laundering [and] terrorist financing'.[25] Moreover, LEAs must be able to pursue parallel investigations into terrorist financing, money laundering and associated predicate offences.[26] The exchange of information between LEAs, as well as private and public sector organisations, has been described as 'critical' and 'crucial' in the fight against money laundering and terrorism financing.[27] Indeed, the FATF notes, 'effective information-sharing is the cornerstone of a well-functioning AML/CTF framework'.[28] The value of sharing intelligence has been demonstrated by recent trends towards expanding information sharing initiatives between LEAs and the private sector for AML/CTF purposes in a number of countries, including the UK, the United States of America (US), Singapore, the Netherlands and Canada.[29] To ensure compliance with its Recommendations, FATF members are subject to a peer-review process, with MERs recording the level of compliance.[30] The MERs are independent 'in-depth country reports analysing the implementation and effectiveness of measures to combat money laundering and terrorist financing'.[31] The FATF uses two components to determine the levels of compliance – effectiveness and technical compliance. However, in light of the UK MER, the suitability of the regime is questionable.

[24] ibid, Part G, Recommendations 36-40.
[25] ibid, Recommendation 2.
[26] ibid, Recommendation 30.
[27] Financial Action Task Force, *Private Sector Information Sharing* (Financial Action Task Force 2017) 2 and European Commission, *Public Consultation on Guidance on the Rules Applicable to the Use of Public-Private Partnerships in the Framework of Preventing and Fighting Money Laundering and Terrorist Financing* (European Commission 2021) p.3.
[28] ibid.
[29] Law Commission (n 10) p.171.
[30] Financial Action Task Force (n 4).
[31] FATF, 'Mutual Evaluations' <https://www.fatf-gafi.org/publications/mutualevaluations/more/more-about-mutual-evaluations.html?hf=10&b=0&s=desc(fatf_releasedate)> accessed May 10 2022.

In 2018, the FATF rated the UK's AML/CTF regime as the best in world.[32] In order to achieve this rating, the UK adopted an aggressive AML/CTF strategy.[33] The legislative measures include the introduction of a comprehensive AML legislative framework that exceeds the international standards.[34] The UK has an established and robust CTF regime, which is regarded as international best practice.[35] HM Government (HMG) stated, 'the findings of the MER showed that the UK has the strongest overall AML/CTF regime'.[36] The UK was regarded as compliant with all Recommendations relating to information exchange. However, this paper questions these findings below, by providing two novel case studies, which demonstrate the weaknesses in the UK's approach to exchanging information for the purposes of combating financial crime. Before doing so, the paper also examines the OECD's promotion of information exchange to combat financial crimes.

The Organisation for Economic Cooperation and Development

The OECD is the international standard-setter relating to international taxation and tax evasion.[37] Similarly to the FATF, the OECD has also promoted the exchange of information as a crucial tool in combatting tax evasion. Indeed, the OECD requires countries to enact both international cooperation mechanisms and an effective framework for domestic inter-agency cooperation as part of its Ten Global Principles in Fighting Tax Crimes.[38] The OECD first

[32] Financial Action Task Force (n 6) p.100.
[33] The HM Treasury Select Committee noted that prior to the publication of the Fourth Mutual Evaluation Report in 2018, 'the pace of reform in this area [money laundering and terrorism financing] has increased'. See HM Treasury Select Committee, *Economic Crime - Anti-money Laundering Supervision and Sanctions Implementation* (HC 2017-19, 2010-I).
[34] See generally HM Government, *Economic Crime Plan 2019-22* (HM Government 2019) and HM Government, *Economic Crime Plan 2023-2026* (HM Government 2023).
[35] Financial Action Task Force, Anti-money Laundering and Counter-terrorist Financing Measures United Kingdom Mutual Evaluation Report (Financial Action Task Force 2018) pp.85-108.
[36] HM Government (n 7) p.17.
[37] OECD, 'Who We Are' <https://www.oecd.org/about/> accessed June 16 2022.
[38] OECD, *Ten Global Principles in Fighting Tax Crime* (2nd edn, OECD 2021).

promoted the international exchange of information through model bilateral Double Taxation Conventions containing an exchange of information provision,[39] followed by bespoke Tax Information Exchange Agreements,[40] and the OECD/Council of Europe Multilateral Convention on Mutual Administrative Assistance in Tax Matters.[41] Despite the possibility of several forms of information exchange under these agreements, the most prevalent was the exchange of information on request, whereby a country requests information from another for the enforcement of its tax laws.[42] Following the financial crisis, the OECD successfully encouraged most of the developed world to commit to the then international tax standard.[43] However, states started to become despondent with this system, with the exchange of information on request increasingly being perceived as an ineffective tool in combatting tax evasion.[44] Consequently, the US enacted the Foreign Account Tax Compliance Act, which compelled countries to provide for the automatic exchange of information relating to accounts held by US citizens offshore.[45] Thereafter, the automatic exchange of information was endorsed by the G20 Finance Ministers, Central Bank Governors,[46] and G20 Leaders as the new international tax standard.[47] As a result, the OECD began to develop the measures that

[39] OECD, *Model Tax Convention on Income and on Capital* (OECD 2017), Article 26.
[40] OECD, *Agreement on Exchange of Information in Tax Matters* (OECD 2002).
[41] Convention on Mutual Administrative Assistance in Tax Matters, as Amended by the 2010 Protocol (entered into force 1 June 2011) 3013 UNTS 1.
[42] M Lang, *Introduction to the Law of Double Taxation Conventions* (2nd edn, IBFD, Linde Verlag GmbH 2014) para 527.
[43] In 2009, the OECD achieved widespread compliance by categorising countries into a white, black and grey list, depending on their level of commitment to the then international tax standard. By the time the final version was published, only four countries, Costa Rica, Malaysia, the Philippines and Uruguay, appeared on the blacklist. OECD, 'A Progress Report on the Jurisdictions Surveyed by the OECD Global Forum in Implementing the Internationally Agreed Tax Standard' (April 2 2009) <https://www.oecd.org/tax/exchange-of-tax-information/42497950.pdf> accessed May 14 2022.
[44] See MJ McIntyre 'How to End the Charade of Information Exchange' [2009] Tax Notes International 255.
[45] FATCA provisions are named after the Act they were originally introduced by - Foreign Account Tax Compliance Act, H.R. 3933, 111th Cong. § 101 (2009); They were subsequently enacted in the Hiring Incentives to Restore Employment Act, H.R. 2847, 111th Cong. §§ 501, 511 (2010), which added chapter 4 of Subtitle A s1471-1474 to the US Internal Revenue Code.
[46] G20 Finance Ministers and Central Bank Governors, 'Communiqué: G20 Meeting of Finance Ministers and Central Bank Governors' (Washington DC, April 19 2013) <http://www.g20.utoronto.ca/2013/2013-0419-finance.html> accessed May 14 2022.
[47] G20, 'G20 Leaders' Declaration' (St Petersburg, September 6 2013) <http://www.g20.utoronto.ca/2013/2013-0906-declaration.html> accessed May 14 2022.

would need to be taken to effect the new standard,[48] eventually publishing the Common Reporting Standard (CRS) and a Model Competent Authority Agreement.[49] Following commitment, countries must implement the CRS into domestic law to enable financial institutions to conduct due diligence and report information regarding their foreign account holders to the national competent authority.[50] The competent authority must then exchange this information with the account holder's country of residence, under the authority of a legal instrument permitting the exchange, and either a bilateral or multilateral Competent Authority Agreement.[51] Following the release of the CRS, 49 jurisdictions, including the UK,[52] committed to undertaking the automatic exchange of information in 2017, and 51 jurisdictions committed to undertaking the first exchanges in 2018.[53]

The automatic exchange of information is a 'game changer' in combatting offshore tax evasion.[54] Unlike the previous system for the exchange of information on request, the country concerned does not need to possess any evidence or indication of an individual's noncompliance; rather, it will receive information regarding accounts held by all of its residents offshore on an automatic basis, thereby facilitating both the detection and deterrence of tax evasion. The OECD has been successful in achieving near-universal commitment to the CRS, which is essential to prevent tax evaders from relocating funds to non-compliant jurisdictions.[55] The CRS has had a significant impact on the amount of wealth held offshore, with the OECD

[48] OECD, *Automatic Exchange of Information: What It Is, How It Works, Benefits, What Remains to be Done* (OECD 2012) and OECD, *A Step Change in Transparency: Delivering a Standardised, Secure and Cost Effective Model of Bilateral Automatic Exchange for the Multilateral Context* (OECD 2013).
[49] OECD, *Standard for Automatic Exchange of Financial Account Information in Tax Matters* (OECD 2014).
[50] ibid p.14.
[51] OECD (n 49).
[52] The UK implemented the CRS via the International Tax Compliance Regulations 2015, SI 2015/878; The International Tax Compliance (Amendment) (No 2) (EU Exit) Regulations 2020, SI 2020/1300.
[53] OECD, 'AEOI: Status of Commitments' (January 5 2022) <https://www.oecd.org/tax/transparency/AEOI-commitments.pdf> accessed May 14 2022.
[54] A Pross et al, 'Turning Tax Policy into Reality – Global Tax Transparency Goes Live' (2017) 27 Int'l Tax Rev 16, 16.
[55] ibid p.17.

noting that bank deposits in international financial centres decreased by 34%, or $551 billion, over the last decade with the automatic exchange of information responsible for 20-25% of that decline.[56] The OECD also claims that €95 billion in additional revenue has been recovered globally from compliance initiatives preceding the CRS.[57] In 2019, HMRC announced that it had received 5.67 million records since implementing the CRS, relating to 3 million UK resident individuals, or entities they control, and since 2010 had raised over £2.9 billion through combatting offshore tax evasion.[58] However, it is unlikely that the entire estimated amount is directly attributable to the CRS, as these estimates include sums raised through other mechanisms.[59] Nonetheless, the implementation of the CRS in the UK has led to the collection of substantial amounts of revenue, likely in excess of initial predictions of £75 million to £270 million annually.[60]

The OECD also emphasises the importance of domestic LEA cooperation and information exchange, noting that there are 'substantial gains to be made by developing strong legal, institutional, operational, and cultural frameworks for tax authorities to report and share information [to prevent] money laundering and terrorist financing'.[61] The OECD advocates for a 'whole of government approach where tax authorities have a key role in not only identifying tax evasion, but also, in identifying and reporting other suspected serious crimes [such as

[56] OECD, *OECD Secretary-General Report to G20 Finance Ministers and Central Bank Governors* (OECD 2019) p.7.
[57] ibid.
[58] HM Revenue & Customs, HM Treasury, 'No Safe Havens 2019: HMRC's Strategy for Offshore Tax Compliance' (May 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/802253/No_safe_havens_report_2019.pdf> accessed May 14 2022.
[59] ibid.
[60] HM Revenue & Customs, 'Tax Administration: Regulations to Implement the UK's Automatic Exchange of Information Agreements' (Impact Assessment, March 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/413976/TIIN_8148_tax_admin_automatic_exchange.pdf> accessed May 4 2022.
[61] OECD, *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors* (OECD 2019) p.11.

money laundering and terrorist financing]'.[62] The OECD's conclusions are supported by typologies of terrorism financing, which reveal strong evidence of terrorists committing tax crimes to finance their activities.[63] Moreover, tax crimes, such as VAT fraud, have been persistently linked to both terrorists and organised criminals, demonstrating the need for a coordinated response.[64] As with the FATF Recommendations, the UK is considered fully compliant with the OECD exchange of information guidelines.[65] Nevertheless, the following case studies demonstrate the weaknesses in the UK's approach to exchanging information for the purposes of combating financial crime.

Part II – Case Studies

This section illustrates a series of deficiencies in the UK's legal framework that enables LEAs to obtain and exchange information by presenting two case studies. In practice, there are inherent flaws in the UK's ability to obtain and exchange of information to detect and address financial crimes. Each case study is divided into three parts and focuses on the legal provisions, highlighting the inadequacies of the exchange of information between LEAs before making a series of recommendations for policy makers. The first case study on terrorism financing and fraud presents evidence that questions the appropriateness of the reporting obligations by examining three terrorist attacks – London (July 7 2005), Manchester Arena (May 22 2017),

[62] OECD, *Improving Co-operation Between Tax and Anti-Money Laundering Authorities: Access by Tax Administrations to Information Held by Financial Intelligence Units for Criminal and Civil Purposes* (OECD 2015) p.5.
[63] See for instance, F Perri and R Brody 'The Dark Triad: Organized Crime, Terror and Fraud' (2011) 14(1) Journal of Money Laundering Control 44, M Freeman 'The Sources of Terrorist Financing: Theory and Typology' (2011) 34(6) Studies in Conflict & Terrorism 461, A Irwin, KK Choo and L Liu 'An Analysis of Money Laundering and Terrorism Financing Typologies' (2012) 15(1) Journal of Money Laundering Control 85 and J Vittori, *Terrorist Financing and Resourcing* (Palgrave MacMillan 2011).
[64] Financial Action Task Force, *Covid-19-Related Money Laundering and Terrorist Financing* (Financial Action Task Force 2020) p.16.
[65] OECD, *Global Forum on Transparency and Exchange of Information for Tax Purposes, Peer Review of the Automatic Exchange of Financial Account Information 2021* (OECD 2021).

and the London Bridge (June 3 2017). The evidence presented here illustrates that UK has not met the requirements of Recommendation 31, yet interestingly, the 2018 FATF MER concluded that here 'all criteria are met. Recommendation 31 is rated compliant'.[66]

Case Study 1 – Terrorism Financing and Fraud

The first case study identifies a link between terrorism financing and fraud, and it then moves on to demonstrate weaknesses within the CTF and fraud reporting obligations, financial intelligence and the exchange of information.

Legal Framework

The Terrorism Act 2000 (TACT) makes it a criminal offence to fail to disclose knowledge or suspicion of another person that has committed a terrorist financing criminal offence.[67] Such a failure to disclose information is identical to the offence of failing to disclose suspicions of money laundering under the Proceeds of Crime Act 2002 (POCA).[68] An individual or organisation who suspects that an offence has been committed under the TACT is legally required to complete a SAR. The courts have defined 'suspicion' as 'being beyond mere speculation and based on some foundation, for example: a degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation'.[69] In *R v Da Silva*, the court stated that,

[66] ibid p.226.
[67] Terrorism Act 2000, s.19.
[68] Proceeds of Crime Act 2002, ss.330–32.
[69] Financial Services Commission, *Guidance Notes – Systems of Control to Prevent the Financial System from Being Used for Money Laundering or Terrorist Financing Activities* (Financial Services Commission 2011) 8.1.

> the essential element of the word 'suspect' and its affiliates … is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice. But the statute does not require the suspicion to be 'clear' or 'firmly grounded and targeted on specific facts' or based upon 'reasonable grounds'.[70]

Moreover, *K v National Westminster Bank, HMRC, SOCA*,[71] determined that the interpretation of suspicion is the same in civil law as it is in criminal law. Applying case law, we therefore have what is often referred to as the 'more than fanciful possibility test'.[72] However, the overall effectiveness of this SAR regime has been called into question. As demonstrated by the Law Commission, its deficiencies include an ineffective SARs database, weak monitoring of enforcement outcomes, inadequate training and a lack of governmental support.[73]

Additionally, the TACT contains a number of statutory measures related to financial information orders. For example, TACT 'deals with orders empowering the police to require financial institutions to supply customer information relevant to terrorist investigation'.[74] An application for an order can be made by a police officer that could 'require a financial institution [to which the order applies] to provide customer information for the purposes of the investigation'.[75] The order could apply to '(a) all financial institutions, (b) a particular description, or particular descriptions, of financial institutions, or (c) a particular financial institution or particular financial institutions'.[76] If a financial institution fails to comply with

[70] *R v DA Silva* [2006] EWCA Crim 1654.
[71] *K v National Westminster Bank, HMRC, SOCA* [2006] EWCA Civ 1039.
[72] Financial Services Commission (n 69).
[73] Law Commission (n 10).
[74] Terrorism Act 2000, Schedule 6.
[75] ibid.
[76] ibid.

the financial information order it is guilty of a criminal offence.[77] The financial institution, however, does have a defence to breaching the financial information order when they can illustrate '(a) that the information required was not in the institution's possession, or (b) that it was not reasonably practicable for the institution to comply with the requirement'.[78] Additionally, the TACT permits the use of account monitoring orders.[79] Judges can grant an account monitoring order if they are satisfied that '(a) the order is sought for the purposes of a terrorist investigation, (b) the tracing of terrorist property is desirable for the purposes of the investigation, and (c) the order will enhance the effectiveness of the investigation'.[80] When an application is made for account monitoring, the order must contain information relating to accounts of the person who is subject to the order.[81]

One of the most important developments in financial intelligence, alongside the SARs regime, is the voluntary exchange of information. The success of information sharing rests on the relationship between LEAs and reporting entities, which in the UK has been 'plagued by mistrust resulting in poor information sharing where vital information possessed by each party has been kept in silos'.[82] In order to address these weaknesses, the Joint Money Laundering Intelligence Taskforce (JMLIT) was established as a private/public partnership between LEAs and the financial sector.[83] JMLIT has 'made very quick progress in aiding voluntary information sharing … and has quickly demonstrated [its] … benefits'.[84] JMLIT has enabled

[77] ibid.
[78] ibid.
[79] ibid.
[80] Terrorism Act 2000, Schedule 6(5).
[81] ibid.
[82] See Home Office, 'Home Secretary on the Work of the Financial Sector Forum: Theresa May Announces Launch of Joint Money Laundering Intelligence Taskforce' (February 24 2015), accessed from <www.gov.uk/government/speeches/home-secretary-on-the-work-of-the-financial-sector-forum> accessed March 4 2023.
[83] National Crime Agency, 'National Economic Crime Centre', (n/d) <www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed March 4 2023.
[84] Financial Conduct Authority, 'Effectiveness and Proportionality: Our Financial Crime Priorities – Speech by Rob Gruppetta, Head of Financial Crime Department' (November 10 2016)

the UK to become a global leader in the exchange of information between reporting entities and LEAs; the UK model has been adopted in Australia,[85] Singapore[86] and Hong Kong.[87] Indeed, the FATF noted, 'JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015 and is considered to be an example of best practice'.[88]

The exchange of information has also been facilitated by the Criminal Finances Act 2017, which permits 'voluntary disclosures within the regulated sector'.[89] The Criminal Finances Act 2017 allows the regulated sector to 'share information with each other on a voluntary basis in relation to a suspicion that a person is engaged in money laundering [or]… terrorist financing'.[90] Information sharing can either be instigated by the regulated sector or the NCA.[91] The provision supports the pre-existing statutory provisions introduced by the Crime and Courts Act 2013, which permits reporting entities to act as information gateways to facilitate the exchange of information between the private sector and LEAs.[92] The FATF has described this as a 'strong feature of the system … [that] enables any person across the public or private sector to voluntarily share information with the NCA'.[93] Information provided via such

<www.fca.org.uk/news/speeches/effectiveness-proportionality-financial-crime-priorities> accessed March 4 2023.

[85] AUSTRAC, 'Fintel Alliance', (n/d) <www.austrac.gov.au/about-us/fintel-alliance> accessed March 4 2023.

[86] Monetary Authority of Singapore, 'CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes' (April 24 2017) <www.mas.gov.sg/News-and-Publications/Media-Releases/2017/CAD-and-MAS-Partner-Industry-Stakeholders-to-Fight-Financial-Crimes.aspx>, accessed March 4 2023.

[87] Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce Launched' (May 26 2017) <www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml> accessed March 4 2023.

[88] Financial Action Task Force (n 6) p.6.

[89] Criminal Finances Act 2017, s.11. This Act introduced this measure into the Proceeds of Crime Act 2002, s.339ZB–ZG and the Terrorism Act 2000, s.21CA–CF.

[90] Home Office, *Home Office Circular: Criminal Finances Act 2017 Money Laundering: Sharing of Information within the Regulated Sector Sections 339ZB-339ZG* (Home Office 2018) p.1.

[91] ibid.

[92] Crime and Courts Act 2013, s.7.

[93] Financial Action Task Force (n 6) p.57.

mechanisms is contained within what are known as 'Super SARs'.[94] Two further information sharing pathways – the Financial Crime Information Network and the Shared Intelligence Service, both of which are hosted by the FCA – enable the sharing of information between LEAs and financial regulatory agencies.[95]

All of these mechanisms are voluntary and reporting entities can decline an invitation to exchange information. Of course, information sharing, and increased co-operation can result in more comprehensive financial profiles of customers that enable financial investigators to focus on certain financial instruments and transactions. Notwithstanding the acclaim it has enjoyed, the JMLIT has attracted some criticism on account of its composition. For example, the FATF has noted that 'some stakeholders felt disenfranchised by their exclusion from it. Many felt that … JMLIT [should be] expanded [to allow] greater dissemination of information'.[96] Another criticism has been that the JMLIT does not engage with reporting entities that are particularly vulnerable to abuse by money launderers; It seemingly focuses exclusively on working with the financial services sector while ignoring other professions, such as accountants,[97] lawyers,[98] and estate agents.[99] The Law Commission concluded that the JMLIT's remit should be extended to include a broader range of reporting entities from the entire regulated sector in order to 'provide a better understanding of relevant intelligence through the sharing of information across multiple sectors'.[100] In response, the NCA stated,

---

[94] Law Commission (n 10) p.44. It is likely that these provisions will be expanded in the forthcoming Economic Crime and Corporate Transparency HC Bill (2022-23) 154.
[95] HM Treasury, 'Call for Information: Anti-Money Laundering Supervisory Regime' (16 March 2017) <www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime>, accessed March 4 2023.
[96] Financial Action Task Force (n 6) p.165.
[97] HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (HM Treasury and Home Office 2017) ch. 6.
[98] ibid chapter 7. See also Financial Action Task Force, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (Financial Action Task Force 2013).
[99] See HM Government, 'Estate Agents Targeted in Money Laundering Crackdown' (March 4 2019) <www.gov.uk/government/news/estate-agents-targeted-in-money-laundering-crackdown>, accessed March 14 2023.
[100] Law Commission (n 10) p.174.

'we do not believe that a simple expansion of the current JMLIT would be … effective'.[101] Conversely, the City of London Police suggested that the JMLIT could contain a number of 'sub-sets … concentrating on different sectors thereby allowing full access or the ability for the JMLIT to co-opt additional members'.[102] Although the creation of the JMLIT and the resultant information sharing has achieved some notable successes, it now seems necessary for HMG to widen the scope of the information sharing model to include other industries, such as social media platforms.[103] The next section illustrates the weaknesses in the UK's approach towards the exchange of information by referring to three terrorist attacks.

London July 7 2005

In 1995, HMRC connected several suspected frauds with Shahzad Tanweer, one of the July 2005 terrorists, yet this information was not disclosed to the FIU or the Security and Intelligence Service (SIS).[104] The group linked to Tanweer gained approximately £8billion from VAT and benefit frauds, of which it sent '1% of its gains, or £80 million to al-Qaeda'.[105] HMRC officials 'were prevented from sharing intelligence with SIS due to its desire to keep tax records confidential'.[106] However, the Anti-terrorism, Crime and Security Act 2001 permits the disclosure of information held by HMRC and provides that 'no obligation of secrecy … prevents the voluntary disclosure of information … to assist any criminal investigation … the section *allows* [author's emphasis] for disclosure to the intelligence services … in support of

[101] ibid p.44.
[102] Law Commission (n 10) p.166.
[103] Ryder (n 10) pp.687-692.
[104] It has been suggested that HMRC became aware of the tax fraud scheme as early as 1995. See T Harper and M Macaskill 'Glaswegian in £300m Fraud Linked to Bin Laden' (April 14 2019) <https://www.thetimes.co.uk/article/glaswegian-in-300m-fraud-linked-to-bin-laden-x707d09pk?region=global> accessed March 4 2023.
[105] S Williams '£80m of British taxpayers' money 'funnelled to al-Qaeda' in decades-long scam' (March 31 2019), <https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled_al-qaeda-decades-long> accessed March 1 2023.
[106] ibid.

their functions'.[107] However, the ability of HMRC to disclose information is restricted by the Commissioners for Revenue and Customs Act 2005, which provides that information must not be disclosed to anyone unless the person making the disclosure has the authority to do so.[108] This applies to HMRC providing information to government departments, LEAs, FIUs and other public bodies. This restriction does not apply if the disclosure is 'made for the purposes of a criminal investigation or criminal proceedings relating to a matter in respect of which the Revenue and Customs have functions'.[109] HMRC's duty of confidentiality is also 'subject to any other enactment permitting disclosure',[110] and many legal gateways have been enacted to provide for the exchange of information between HMRC and LEAs. The Counter Terrorism Act 2008 provides that 'a person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions'.[111] Additionally, the Money Laundering Regulations provide that HMRC as a 'supervisory authority which, in the course of carrying out any of its supervisory functions or otherwise, knows or suspects, or has reasonable grounds for knowing or suspecting, that a person is or has engaged in money laundering or terrorist financing *must* [author's emphasis] as soon as practicable inform the NCA'.[112] Between 2021 and 2022 the HMRC Economic Crime Supervision 'continued to submit SARs to the NCA in line with its regulatory obligations in respect of SARs that are relevant to the supervisory activity'.[113] They added that it:

[107] Anti-terrorism, Crime and Security Act 2001, s.19.
[108] Commissioners for Revenue and Customs Act 2005, s.18(1).
[109] ibid, s.18(2)(d).
[110] ibid, s.18(3).
[111] Counter Terrorism Act 2008, s.18(1).
[112] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 46(5).
[113] HM Revenue and Customs 'Corporate Report – HMRC Economic Crime Supervision Annual Assessment Report: 1 April 2021 to 31 March 2022' (October 6 2022) <https://www.gov.uk/government/publications/hmrc-economic-crime-supervision-annual-assessment-report-2021-to-2022/hmrc-economic-crime-supervision-annual-assessment-report-1-april-2021-to-31-march-2022#information-sharing-between-supervisors-and-public-authorities> accessed March 4 2023.

> ‘has also worked to increase its interactions and close working with the NCA … in relation to SAR submissions and has worked with [the FIU] … to look at when reporting is relevant and required to ensure the best use of intelligence sharing within the Regulations … to ensure that intelligence … is not duplicated, creating potential resourcing impacts for any party in the process’.[114]

HMRC, in its capacity as a supervisory authority under the Money Laundering Regulations, has potentially breached Regulation 46(5) by not submitting a DATF SAR to the NCA. However, it is unlikely that HMRC will be subjected to a civil penalty for breaching the Money Laundering Regulations because they are imposed by statutory supervisory authorities on the regulated sector, not on statutory supervisory authorities. Furthermore, HMRC will not be exposed to any disciplinary action by the Office for Professional Body AML Supervising which supervises professional body supervisors in the legal and accountancy sectors.[115] Additionally, HMRC also has a ‘duty to co-operate’ and ‘disclosure’ under the Money Laundering Regulations,[116] which provide that ‘co-operation may include the sharing of information which the supervisory authority is not prevented from disclosing’.[117] The decision by HMRC not to disclose the information, despite several mechanisms facilitating the exchange of information is problematic for this information would have provided intelligence on the financing of the terrorist attack and could potentially have prevented its commission. The difficulty is not with the legislation or guidance, but the restrictive interpretation of ‘taxpayer confidentiality’. HMRC practice is not in line with national, regional, and international legal instruments, thus

[114] ibid.]
[115] Financial Conduct Authority ‘Office for Professional Body Anti-Money Laundering Supervision (OPBAS)’ (January 23 2018) <https://www.fca.org.uk/about/how-we-operate/who-work-with/opbas> accessed March 4 2023.
[116] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 50 and 52.
[117] ibid, Regulation 50(3).

illustrating that the reporting obligations are not suitable and questioning the findings of the 2018 MER.

Manchester Arena May 22 2017

In order to commit the terrorist attack in the Manchester Arena in 2017, Salman Abedi used student loans and his maintenance grant.[118] Abedi received £7,000 from the Student Loans Company after securing a place on a degree at Salford University in October 2015. An investigation by the European Commission estimated that Abedi had received up to $18,000 in student loans and other benefit payments.[119] The Student Loan Company paid £1,000 into Abedi's account at the start of January 2017 and a further £2,258 at the end of that month. The money from the student loan was withdrawn in regular amounts of up to £300.[120] It is interesting to note that Abedi continued to receive funds from the Student Loan Company even though he had stopped attending classes at Salford University.[121] The Money Laundering Regulations do not apply to higher education institutions (HEIs), only the regulated sector,[122] and HEIs have a limited legal obligation to report any suspicions of fraud or terrorism financing to the NCA.[123] Theoretically, HEIs could be regarded as a High-Value Dealer for the reporting obligations to apply. The term is defined as 'a firm or sole trader who by way of business trades in goods … when the trader makes or receives, in respect of any transaction, a payment or

[118] 1 R Mendick 'Manchester suicide bomber used student loan and benefits to fund terror plot' (May 27 2017), <https://www.telegraph.co.uk/news/2017/05/26/exclusive-manchester-suicide-bomber-usedstudent-loan-benefits/> accessed March 2 2023.
[119] European Commission Study on an EU initiative for a restriction on payments in cash (Brussels: European Commission, 2017) p 42.
[120] P Stubley 'Hashem Abedi Trial: Benefits Claimed by Manchester Bomber's Family Were Used in Terror Plot Jury Hears' The Independent (February 10 2020) <https://www.independent.co.uk/news/uk/crime/manchester-arena-bombing-benefits-family-samia-abedi-hashem-trial-a9327816.html.
[121] European Commission, (n 119).
[122] The Money Laundering, Terrorist Financing Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 8(2).
[123] N Ryder, S Bourton, H Hillman and D Hall, 'Higher Education Institutions and Money Laundering', (Wales Fraud Forum Annual Conference, Cardiff, September 2022).

payments in cash of at least 10,000 euros in total'.[124] However, a survey of the application of the reporting obligations to the HEIs noted that only 2 out of 110 respondents considered themselves to be high value dealers.[125] Therefore, the uncertainty surrounding the application of the reporting obligations to HEI illustrates further weaknesses in the exchange of information.

London Bridge June 3 2017

The terrorist attacks in London in June 2017, illustrates deficiencies in the use of DATF SARs and the reporting obligations.[126] Here, one of the terrorists, Khuram Butt, was investigated and arrested on suspicion of falsely reporting fraudulent activity (£3,300),[127] on three bank accounts in October 2016.[128] It was alleged that Butt had been making 'unauthorised withdrawals from his accounts, with Santander, and then pocketing the refunds'.[129] Indeed, in preparation for the terrorist attack, Butt emptied his two other bank accounts (Nationwide and Lloyds) and had successfully applied for two loans (totalling £14,000).[130] After his arrest, Butt was granted bail and the fraud charges were eventually dropped due to insufficient evidence.[131] The Intelligence and Services Committee (ISC) stated that 'during Butt's arrest … counter-terrorism police had discovered files that it considered "may be successfully used in a prosecution under the

[124] The Money Laundering, Terrorist Financing Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, Regulation 14.
[125] Ryder *et al*, above (n 123).
[126] D Anderson, *Attacks in London and Manchester March-June 2017: Independent Assessment of MI5 and Police* (HM Government, 2017) p.1.
[127] M White 'London Bridge Attack: MI5 Accused of "Damning List" of Failures' (June 28 2019)<https://news.sky.com/story/london-bridge-attack-mi5-accused-of-damning-list-of-failures-11750204> accessed March 4 2023.
[128] Intelligence and Security Committee, *The 2017 Attacks: What Needs to Change? Westminster, Manchester Arena, London Bridge, Finsbury Park, Parsons Green* (Intelligence and Security Committee, 2018) p.85.
[129] London Bridge Inquests, 'Inquests Concerning the Attackers Day 6A' (July 9 2019)<https://londonbridgeinquests.independent.gov.uk/wp-content/uploads/2019/07/LBI-Day-6A.pdf> accessed March 4 2023.
[130] ibid, pp.42, 43, 66 and 67.
[131] London Bridge Inquests, above (n 129) p. 41. Also, see Intelligence and Security Committee, above (n 128), p.85.

Terrorism Act"; however … the issue was not explored further'.[132] The ISC noted that 'in July 2016, there was a potential disruption opportunity presented by Butt's suspected engagement in bank fraud, and counter terrorist police arrested Butt in October 2016. However, by June 2017 it was decided that no further action could be taken, due to a lack of evidence'.[133] Similarly, Anderson noted that,

> while under investigation by MI5, Khuram Butt was arrested for fraud in October 2016 and granted bail. He had not yet been told by 3 June 2017, the date of the attack that on 1 June the decision had been taken not to prosecute him.[134]

Here, Santander was under no legal obligation to submit a SAR to the NCA concerning attempted fraud.[135] Therefore, the reporting obligations are unfit to track and prevent terrorist financing through fraud. Clearly, the exchange of information mechanisms as they currently stand are therefore unsatisfactory.

Recommendations

There are inherent flaws in the UK's ability to obtain and exchange information to detect fraud and terrorism financing. In light of this assessment, the following recommendations for reform are put forward. Firstly, HEIs should be part of the regulated sector and tasked with complying with AML/CTF legislation, including the submission of SARs. This should provide LEAs with additional financial intelligence to initiate or support terrorism financing investigations.[136]

---

[132] ibid.
[133] Intelligence and Security Committee, above (n 128), p.85.
[134] Anderson, above (n 126), p.17.
[135] See J Goldstraw-White, M Gill, *The Mandatory Reporting of Fraud: Finding Solutions and Sharing Best Practice* (Fraud Advisory Panel, 2021).
[136] Ryder *et al*, above (n 123).

Secondly, the reporting of fraud should become mandatory placing it on the same legislative footing as money laundering and terrorist financing.[137] Therefore, to reduce the risks presented by the this case study, the Fraud Act 2006 could be amended to include a failure to disclose offence based on money laundering and terrorism financing.[138] The offence would be committed under the Fraud Act 2006 for failing to report a suspected fraud where a person 'receives information in the course of a business in the regulated sector … thereby knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in fraud' and 'fails to disclose a nominated officer, or person authorised for by the Director of NCA, the information on which his knowledge or suspicion is based as soon as is practicable after the information comes to him'. These amendments would provide clarity and certainty regarding the nature and extent of the reporting obligations. This approach will result in better intelligence for the policing of fraud. However, if the reporting of fraud does become mandatory, it will lead to an increased administrative and financial burden on reporting entities. HM Treasury recently announced that it would provide an £18million (2022-2023) with an additional £12million (2023-2024) to tackle money laundering and fraud.[139] This funding is further supported by the Economic Crime Levy,[140] which is expected to contribute £100million per year.[141] The impact of the Economic Crime Levy is debatable, because it contains no specific reference towards tackling fraud. Furthermore, the benefits of the additional funding on tackling fraud has been questioned by Spotlight on Corruption who asserted that HMG only

[137] This approach has been adopted in South Africa, the Republic of Ireland and Scotland, ibid, pp.39-41.
[138] See Proceeds of Crime Act 2002, s.330, Terrorism Act 2000, s.19.
[139] HM Treasury, *Autumn Budget and Spending Review 2021: A Stronger Economy for the British People* (HM Treasury, 2021) p.99.
[140] Economic Crime (Anti-Money Laundering) Levy Regulations 2022, SI 2022/26.
[141] The Economic Crime Levey is paid by reporting entitles who are subjected to the AML/CTF reporting obligations. See HM Revenue & Customs, 'Policy paper – Economic Crime (Anti-Money Laundering) Levy' (October 2021), <https://www.gov.uk/government/publications/economic-crime-anti-money-laundering-levy/economic-crime-anti-money-laundering-levy> accessed March 4 2023.

spends 0.042% of GDP, or £852million, on tackling financial crime.[142] The All-Party Parliamentary Groups on Fair Business and Anti-Corruption and Responsible Tax concluded, 'LEAs are outspent and outgunned by criminals and the corrupt'.[143] Indeed, the House of Commons Treasury Committee noted that spending on tacking economic crime needs to be increased.[144] HMG responded by proposing a sustainable funding model totalling 400million.[145] However, the amount of money equates to 0.2% of the extent of fraud of £190billion.[146] In order to address this criticism, there are a number of mechanisms that could be introduced to soften the financial burden on reporting entities. Firstly, HM Treasury and the Home Office could resource and equip LEAs to tackle fraud by providing an additional £300million.[147] Secondly, the additional funding could form part of a cross-governmental Economic Crime Fighting Fund.[148] Thirdly, a proportion of the financial crime penalties received by the FCA should be redistributed towards supporting the additional costs of mandatory reporting of fraud.[149]

Case Study 2 – Tax Evasion

This case study builds on the findings of the first case study and presents further findings that illustrate weaknesses within tax fraud, financial intelligence and the exchange of information.

---

[142] Spotlight on Corruption 'Government Spend Equivalent of Just 0.042% of GDP on Fighting Economic Crime – New Analysis' (January 24 2022) <https://www.spotlightcorruption.org/press-release-government-spends-equivalent-of-just-0-042-of-gdp-on-fighting-economic-crime-new-analysis/> accessed March 4 2023.
[143] All Parliamentary Group on Anti-Corruption & Responsible Tax, *Economic Crime Manifesto* (All Parliamentary Group on Anti-Corruption & Responsible Tax, 2022) p.10.
[144] House of Commons Treasury Committee, *Economic Crime* (House of Commons Treasury Committee, 2022) p.71.
[145] House of Commons Treasury Committee, *Economic Crime: Responses to the Committee's Eleventh Report Eighth Special Report of Session 2021–22* (House of Commons Treasury Committee, 2021) pp.5-6.
[146] National Crime Agency, 'Fraud' (n/d), <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime> accessed March 4 2023.
[147] Parliamentary Group on Anti-Corruption & Responsible Tax, above (n 143).
[148] ibid.
[149] There is precedent for HM Treasury diverting funds from financial penalties received by the FCA. See, HM Government, 'LIBOR Fines to be Used to Support Military Charities and Royal Voluntary Service' (July 2016), <https://www.gov.uk/government/news/libor-fines-to-be-used-to-support-military-charities-and-royal-voluntary-service> accessed March 6 2023.

Legal Framework

Financial intelligence is essential in combatting tax evasion, for information is crucial to verify the claims made by taxpayers and to detect any noncompliance with tax legislation. The methods used by HMRC to obtain financial intelligence in tax evasion cases depends on whether it has chosen to pursue a civil or criminal investigation. In cases where HMRC suspect fraud, yet decide against conducting a criminal investigation, it is likely that Code of Practice 9 (CoP9) will be used to investigate the suspected fraud. CoP9 is a procedure whereby HMRC offer the suspect the opportunity to disclose their fraudulent conduct via a Contractual Disclosure Facility, in exchange for a guarantee that the individual will not face criminal investigation or prosecution.[150] HMRC uses Code of Practice 8 (CoP8) to resolve 'cases where the CoP9 is not used'.[151] Although CoP8 used to be restricted to cases not concerning fraud, including failed tax avoidance schemes, it now extends to cases that involve potential criminal conduct.[152] HMRC's Criminal Investigation Policy currently provides that it prefers

> to deal with fraud by use of the cost-effective civil fraud investigation procedures under Code of Practice 9 wherever appropriate. Criminal investigation will be reserved for cases where HMRC needs to send a strong deterrent message or where the conduct involved is such that only a criminal sanction is appropriate.[153]

[150] HM Revenue & Customs, 'Code of Practice 9: HM Revenue & Customs Investigations Where We Suspect Fraud' (June 2014) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/494808/COP9_06_14.pdf> accessed April 10 2023.
[151] HM Revenue & Customs, 'HM Revenue and Customs Fraud Investigation Service – Code of Practice 8' (February 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/684324/COP8_02_18.pdf> accessed April 10 2023.
[152] A Wells, 'No, No, No!' (2010) 166(4272) Taxation 6, 7; R Brockwell, L McKeown, 'No More Mr Nice Guy?' (2003) 151(3913) Taxation 350.
[153] ibid.

Following the merger of HM Customs and Excise and the Inland Revenue, HMRC's criminal investigation powers were aligned with the police investigation powers contained in the Police and Criminal Evidence Act (PACE) 1984.[154] As a result, HMRC's powers are now aligned with those in use in the wider criminal justice system. HMRC have the power to request document production orders either under PACE, where the material requested is 'special procedure material',[155] or otherwise under its preserved production powers relating to the type of tax at issue.[156] These powers enable HMRC to request documents from third parties when there are reasonable grounds to suspect tax fraud.[157] The powers are designed to prevent searches of property owned by innocent third parties.[158] HMRC similarly has the power to issue disclosure notices, also aimed at third parties, under the Serious Organised Crime and Police Act 2005.[159] Failing to comply or providing false or misleading information in response to the disclosure notice is a criminal offence.[160] HMRC has the power to apply for search warrants and execute seizures under PACE,[161] and the POCA,[162] where there are reasonable grounds for believing that an indictable offence has been committed and the material sought is likely to be of substantial value to the investigation.[163] Relevant HMRC officers can arrest suspects for indictable tax offences and search property following arrest,[164] but may not charge or bail suspects, or take their fingerprints.[165] At all times, HMRC has access to information that is

[154] Finance Act 2007, ss.82-87.
[155] Police and Criminal Evidence Act 1984, Schedule 1, s.14(2).
[156] Taxes Management Act 1970, s.20BA; Value Added Tax Act 1994, Schedule 11, para 11; Finance Act 1994, Schedule 7, para 4A; Finance Act 1996, Schedule 5, para 7; Finance Act 2000, Schedule 6, para 131; Finance Act 2001, Schedule 7, para 8; Finance Act 2003, Schedule 13, Part 6.
[157] ibid.
[158] A Craggs, 'Beware of the Knock' (2017) 180(4617) Taxation 11, 13.
[159] Serious Organised Crime and Police Act 2005, ss.60-70.
[160] ibid s.67.
[161] Police and Criminal Evidence Act 1984, s.8, s.114.
[162] Finance Act 2013, s.224, Schedule 48.
[163] Police and Criminal Evidence Act 1984, s.8, s.114.
[164] Police and Criminal Evidence Act 1984, s.24 and s.32.
[165] Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015, SI 2015/1783, Art 4.

ordinarily available, including government records and social networking sites.[166] In certain cases, HMRC has the power to employ intrusive surveillance powers.[167]

Additionally, tax evasion is a predicate offence for the purposes of the AML framework, with evaded taxation constituting criminal property for the purposes of the POCA 2002.[168] Consequently, SARs must be submitted when it is known or suspected that another is engaged in laundering the proceeds of tax evasion, potentially providing valuable intelligence.[169] HMRC regularly receives reports from the FIU and is the largest recipient of SAR data.[170] Nevertheless, HMRC has been criticised for not making full use of this intelligence,[171] using only just over one percent of the 300,000 reports it received in 2013.[172] HMRC's use of SARs improved with the move to feed SAR data into its CONNECT database, which enables the matching of SAR data with other data held by HMRC.[173] In 2018-19, SAR data assisted HMRC in recovering £40.2 million through civil enquiries and over £30 million from civil

[166] HM Revenue & Customs, 'Guidance: HMRC's Criminal Investigation Powers and Safeguards' (July 2021) <https://www.gov.uk/government/publications/criminal-investigation/criminal-investigation> accessed April 4 2023.
[167] Contained in the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000 and the Police Act 1997.
[168] Proceeds of Crime Act 2002, s.340.
[169] ibid, s.330-332.
[170] Her Majesty's Inspectorate of Constabulary, 'An Inspection of Her Majesty's Revenue and Customs Performance in Addressing the Recovery of the Proceeds of Crime from Tax and Duty Evasion and Benefit Fraud: Revisit 2013' (Her Majesty's Inspectorate of Constabulary, 2014) p.30. HMRC is 'a major user of SAR information' National Crime Agency, 'SARs in Action' (Issue 1, 2019) <https://nationalcrimeagency.gov.uk/who-we-are/publications/268-ukfiu-sars-in-action-march-2019> accessed March 4 2023, at p.7.
[171] Her Majesty's Inspectorate of Constabulary, 'An Inspection of Her Majesty's Revenue and Customs Performance in Addressing the Recovery of the Proceeds of Crime from Tax and Duty Evasion and Benefit Fraud: Revisit 2011' (Her Majesty's Inspectorate of Constabulary, 2011) p.32.
[172] T Monger, 'Pointless POCA?' (2014) 174 Taxation 8.
[173] National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2014* (National Crime Agency, 2015) p.24.

investigations.[174] In 2019-20, these figures declined to £33.5 million and over £15 million respectively.[175]

Despite its extensive information powers, the previous case study demonstrates HMRC's reluctance to exchange information with national LEAs for the purposes of combatting terrorism financing, allegedly owing to 'taxpayer confidentiality'.[176] Indeed, the confidentiality of taxpayer information has received both common law and statutory protection since the inception of the income tax,[177] being considered a 'vital element in the working of the system' of revenue collection.[178] Taxpayer information is currently protected by the CRCA 2005. However, the Act itself does not refer to taxpayer confidentiality; rather, taxpayer confidentiality is considered to be a 'by-product' of s.18, which imposes a duty on HMRC officials not to disclose information received in connection with a function of HMRC.[179] The duty of non-disclosure is supported by the criminal offence in s.19 concerning the wrongful disclosure by HMRC employees of taxpayer identifying information in contravention of s.18. The offence is punishable by up to two years' imprisonment.[180] However, s.18 contains several exceptions to the duty of confidence. For instance, information may be disclosed pursuant to a function of HMRC.[181] This has been interpreted narrowly by HMRC as not permitting the

[174] In addition, 'a further £9,408,865 was generated from enhancing HMRC cases already under civil investigation'. National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2019* (National Crime Agency, 2020) p.11.
[175] 'A further £7,072,085 was generated from enhancing HMRC cases already under civil investigation by providing intelligence in SARs'. See National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2020* (National Crime Agency 2021) p.18.
[176] Williams (n 105).
[177] O Mba, 'Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality' [2012] 2 BTR 187, 187.
[178] *R v Inland Revenue Comrs, Ex p National Federation of Self-Employed and Small Businesses Ltd* [1982] AC 617, 633.
[179] E McNicholas, 'Revenue and Customs Act 2005 — Powers and Disclosure' (2005) 26(20) PTN 153.
[180] Commissioners for Revenue and Customs Act 2005, s.19(4).
[181] ibid, s.18(2)(a)

disclosure of information to Parliamentary committees and inquiries.[182] The term has also been interpreted narrowly by the Supreme Court as only permitting disclosure in accordance with HMRC's primary function of revenue collection, thereby not encompassing 'off the record' disclosures to the media regarding tax avoidance schemes.[183] Information may also be disclosed for the purposes of criminal or civil proceedings, in pursuance of a court order, for the purposes of an inspection, to enforce a devolved tax, or with consent of the person concerned.[184] In regards to disclosure to LEAs, information may also be disclosed to prosecuting authorities,[185] or other authorities if the Commissioners are satisfied that it is in the public interest for information to be disclosed and it is of a kind specified in the subsection.[186] For instance, with consent of the Commissioners, information may be disclosed for the purposes of public safety, or the prevention or detection of crime.[187] However, HMRC note that this exception also applies in 'very limited circumstances'.[188]

Importantly, HMRC's duty of confidentiality is also 'subject to any other enactment permitting disclosure',[189] and many legal gateways have been enacted to provide for the exchange of information between HMRC and other LEAs. For instance, s.19 of the Anti-Terrorism Crime and Security Act 2001 (ATCSA) provides that no obligation of secrecy prevents the disclosure of information for the purposes of any criminal investigation or criminal proceedings, or the initiation or discontinuance of such, in the UK or elsewhere. As such, the ATCSA enables

[182] See for instance, Committee of Public Accounts, *HM Revenue & Customs 2010–11 Accounts: Tax Disputes* (HC 2010–12, 1531-I) Ev 65-67 (written evidence from the Permanent Secretary for Tax, HMRC, October 19 2011).
[183] *R (on the application of Ingenious Media Holdings Plc) v Revenue and Customs Commissioners* [2016] UKSC 54.
[184] Commissioners for Revenue and Customs Act 2005, s.18(2).
[185] ibid, s.18(2)(b), s.21.
[186] ibid, s.18(2)(b), s.20.
[187] ibid, s.20(4)-(6).
[188] HM Revenue & Customs, *HMRC Internal Manual: IDG40340 - Sharing Information Outside of HMRC: Lawful Disclosure: Public Interest Disclosure* (HM Revenue & Customs, 2022).
[189] Commissioners for Revenue and Customs Act 2005, s.18(3).

HMRC to disclose information to LEAs, such as the FCA and the Serious Fraud Office (SFO), for criminal investigation purposes.[190] Additionally, s.19 of the Counter Terrorism Act 2008 permits disclosure to SIS for the purpose of enabling the service to carry out any of its functions. HMRC may also disclose information to the FCA to assist with any of its statutory functions.[191] Despite this plethora of legal gateways, HMRC have persistently failed to proactively share information with LEAs for the purposes of preventing, detecting and combatting crime, as illustrated by the preceding case study.

The reason for HMRC's failure to disclose information thus lies not in the absence of a legal gateway, but rather, in HMRC's application of the CRCA. Following an inquiry into HMRC's approach to settling large tax disputes, in written evidence to the Public Accounts Committee, the then Permanent Secretary for Tax at HMRC explained that the CRCA provides 'a power, rather than an obligation, to disclose'.[192] As the language used in the CRCA is permissive, rather than obligatory, the power rests within HMRC to decide whether or not to disclose information, even in cases of serious organised crime and terrorism.[193] The issue is exacerbated by HMRC's narrow interpretation of the legislative provisions, often leading to an unwillingness to consent to information disclosure.[194] Moreover, there appears to be limited scope for challenging HMRC's interpretation of the CRCA, with a legal challenge by the PAC

[190] HMRC has signed ATCSA MoUs with 25 LEAs, HM Revenue & Customs, *HMRC Internal Manual: IDG50140 - Information Disclosure Gateways with other Government Departments: Anti-Terrorism, Crime and Security Act 2001 (ATCSA): Bodies with whom HMRC has Signed an ATCSA Memorandum of Understanding* (HM Revenue & Customs, 2022) <https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg50140> accessed March 4 2023.
[191] Financial Services and Markets Act 2000, s.350.
[192] Committee of Public Accounts (n 182).
[193] When questioned whether it was remiss of HMRC not to have informed the FCA about allegations concerning HSBC (Suisse), Martin Wheatley, then Chief Executive of the Financial Conduct Authority, replied 'I do not know if they have any such obligation upon them'. Treasury Select Committee, *Financial Conduct Authority Hearings: Oral evidence* (HC 2014-15, 1055).
[194] Committee of Public Accounts (n 182) p.9.

previously blocked purportedly due to a lack of funding.[195] HMRC's interpretation of the CRCA is likely to be influenced by the 'culture of secrecy' that exists within HMRC, which serves to inhibit information exchange.[196] Indeed, in the debates preceding the enactment of the CRCA, the then Paymaster General confirmed the intention was to create a 'culture of taxpayer confidentiality' noting that 'the duty will be drawn to officers' attention and will be emphasised during induction training and in regular messages throughout their career'.[197] Aside from the threat of criminal prosecution, HMRC staff will also be aware of HMRC's prior treatment of whistle-blowers, such as Osita Mba; following disclosure of information regarding improper settlement activities by HMRC Commissioners to the PAC and the Treasury Select Committee, HMRC used intrusive surveillance powers against Mr Mba to investigate false allegations that he had also disclosed information to the media.[198] Accordingly, it is clear that there is a strong culture of secrecy at HMRC, which inhibits the proactive disclosure of information.

In recent years, HMRC appear to have made progress in advancing cooperation with other LEAs. In the wake of the Panama Papers, a multi-agency taskforce was established, the Joint Financial Analysis Centre (JFAC), comprised of the NCA, HMRC, SFO and FCA.[199] JFAC was tasked with investigating the data from the Panama Papers leak. By taking a cooperative approach, JFAC initiated over 30 investigations into individuals suspected of a plethora of financial crimes, including money laundering, tax evasion and corruption, as well as the

[195] M Hodge, *Called to Account: How Governments and Vested Interests Combine to Waste Our Money* (Little Brown 2016).
[196] As Butler notes, 'Secrecy is not merely created by laws but reflects a broader culture'. O Butler, 'Official Secrecy and the Criminalisation of Unauthorised Disclosures' (2022) 138 LQR 273, 276.
[197] Commissioners for Revenue & Customs Bill Deb 11 January 2005, Col 64.
[198] Hodge (n 195).
[199] HM Treasury, Cabinet Office, 'UK Launches Cross-Government Taskforce on the "Panama Papers"' (News Story, 10 April 2016) <https://www.gov.uk/government/news/uk-launches-cross-government-taskforce-on-the-panama-papers> accessed 4 March 2023.

professional enablers of these activities.[200] After investigating the Panama Papers leak, JFAC was tasked with leading LEA exploitation of criminal intelligence on financial crime, particularly, bulk financial data.[201] The functions of JFAC were later taken over by the National Economic Crime Centre (NECC) and the National Data Exploitation Capability (NDEC), housed in the NCA.[202] The NECC is a 'multi-agency centre to bring together LEAs, government departments, regulatory bodies and the private sector with the goal of driving down serious and organised economic crime'.[203] The NDEC is 'a multidisciplinary team including data scientists, intelligence officers and analysts working to enhance the capabilities of the NCA and wider UK law enforcement … to detect and disrupt serious and organised crime'.[204] Accordingly, it appears that UK LEAs, including HMRC, are working more cooperatively to exploit financial intelligence to detect financial crime. However, while HMRC may be willing to share their skills and resources with other LEAs in the investigation of jointly held financial intelligence, the case study above demonstrates HMRC's unwillingness to proactively disclose information that is of interest to other LEAs, which they have discovered in the course of their revenue collection function. While there are important reasons to preserve taxpayer confidentiality, both through legislation and a culture of secrecy at HMRC, taxpayer confidentiality should not be preserved at the expense of detecting serious criminal activities, such as, terrorism. Aside from HMRC's failure to disclose information relating to terrorism financing, the following case study also reveals HMRC's unwillingness to exchange information with LEAs that have been tasked with combatting money laundering and corporate financial crime.

---

[200] Financial Action Task Force (n 6) p.57.
[201] HM Government, 'United Kingdom Anti-Corruption Strategy 2017-2022: Year 3 Update – 2020' (December 16 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041398/2021.12.15_Year_3_Update_to_the_Anti-Corruption_Strategy.pdf> accessed March 4 2023.
[202] ibid.
[203] ibid.
[204] ibid.

HSBC and Tax Evasion

This case study focuses on how following the 2007/2008 financial crisis, and the LIBOR and FOREX scandals, elements of the UK banking sector became embroiled in another financial scandal, tax evasion. In February 2015, whistle-blower Herve Falciani stated that HSBC bank had assisted numerous wealthy clients to evade paying millions of pounds in tax.[205] The International Consortium of Investigative Journalists reported that HSBC Private Bank (Suisse) had persisted in offering its services to customers linked to allegations of bribery, arms trafficking and the sale of blood diamonds. Secondly, that HSBC continued to work for people and institutions that are closely associated with the regimes of Hosni Mubarak, Ben Ali and Bashar al-Assad. Thirdly, there are claims that clients in several jurisdictions benefited from HSBC tax advice and services, leading to tax avoidance and evasion. The allegations suggest that HSBC was more than a passive recipient of funds; HSBC not only set up these accounts, but also, reassured its international clients that details of accounts held would not be disclosed to national authorities.[206] In fact, HSBC wrote to its customers to inform them how to circumvent the European Savings Tax Directive, designed to counter tax evasion,[207] and provided individuals with anonymous credit cards to withdraw funds without detection.[208] Following investigation, it was found that of the leaked accounts held by 106,000 clients in 203 countries, approximately 7,000 clients were based in the UK and of those, 1,100 had not paid the correct amount of tax.[209] HMRC's response to the HSBC scandal was 'seriously

[205] Gerard Ryle et al, 'Banking Giant HSBC Sheltered Murky Cash Linked to Dictators and Arms Dealers', International Consortium for Investigative Journalists (February 8 2015) <https://www.icij.org/investigations/swiss-leaks/banking-giant-hsbc-sheltered-murky-cash-linked-dictators-and-arms-dealers/ > accessed March 4 2023.
[206] ibid.
[207] Council Directive 2003/48/EC of 3 June 2003 on Taxation of Savings Income in the Form of Interest Payments [2003] OJ L 157/38.
[208] BBC News, 'HSBC Bank "Helped Clients Dodge Millions in Tax"' BBC (February 10 2015) <http://www.bbc.co.uk/news/business-31248913> accessed March 4 2023.
[209] ibid.

legally flawed'.[210] Specifically, only one prosecution has been brought against a UK client concerning tax evasion, and no criminal prosecution has been brought by the UK authorities against the bank itself for assisting bank customers with tax evasion and money laundering offences.[211] Despite HMRC's claims to the contrary, this is in sharp contrast to action taken in other jurisdictions, such as France and the US, both of which reached a Deferred Prosecution Agreement with, and imposed significant penalties on, HSBC (Suisse).[212]

It is argued that the key problem was sharing information. Lin Homer, then Chief Executive of HMRC, noted that HMRC could not pursue action against the bank as HMRC was not responsible for investigating allegations of money laundering and was prohibited from sharing information with other LEAs unless used to aid the enforcement of taxation.[213] Indeed, to protect taxpayer confidentiality, the Treaty providing for the exchange of information in tax matters between France and the UK provides that any information received:

> shall be disclosed only to persons or authorities concerned with the assessment or collection of, the enforcement or prosecution in respect of, or the determination of appeals in relation to, the taxes referred to in paragraph 1 … such persons or authorities shall use the information only for such purposes.[214]

---

[210] O Bowcott, 'HSBC Should Face UK Criminal Charges, Says Former Public Prosecutor', *The Guardian* (February 22 2015) <https://www.theguardian.com/politics/2015/feb/22/hsbc-uk-criminal-charges-former-public-prosecutor-hmrc> accessed March 4 2023.
[211] *R v Shanly*, The Times, 5 July 2012 (Wood Green Crown Court).
[212] United States Department of Justice, 'Justice Department Announces Deferred Prosecution Agreement with HSBC Private Bank (Suisse) SA' (December 10 2019) <https://www.justice.gov/opa/pr/justice-department-announces-deferred-prosecution-agreement-hsbc-private-bank-suisse-sa> accessed March 4 2023; MM Hamilton, 'HSBC to Pay $352m to Settle Tax Evasion Charges in France International Consortium of Investigative Journalists (November 15 2017) <https://www.icij.org/investigations/swiss-leaks/hsbc-swiss-france-352m-settlement/> accessed March 4 2023.
[213] Public Accounts Committee, *Oral Evidence: Tax Avoidance and Evasion: HSBC* (23 March 2015, HC 2014-15 1095-I); Public Accounts Committee, *Oral Evidence: Increasing the Effectiveness of Tax Collection: A Stocktake of Progress Since 2010* (11 February 2015, HC 2014-15, 974-I).
[214] Convention between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the French Republic for the Avoidance of Double Taxation and the Prevention of Fiscal Evasion

However, the Treaty is modelled on the OECD's Tax Convention on Income and on Capital, which provides that the Convention 'allows the sharing of tax information by the tax authorities of the receiving State with other LEAs and judicial authorities in that State on certain high priority matters'.[215] Accordingly, information can be exchanged with other LEAs in accordance with the Convention when two conditions are met: the laws of both countries must permit the use of the information for other purposes and the supplying state must authorise such use.[216] HMRC claimed that it asked the French authorities for permission to share the data with other LEAs in 2010; a claim that was disputed France.[217] The activities of HSBC (Suisse) were only revealed to the FCA and other LEAs in 2015, following the dissemination of the information in the media.[218] Following this, HMRC obtained confirmation from the French authorities that restrictions on the use and sharing of the data could be lifted for the purpose of investigating other financial crimes.[219] HMRC later met the SFO, the NCA and the FCA to consider sharing of the data.[220] However, all investigative activities were discontinued.[221] The failure to act against a UK-headquartered bank, which assisted clients to evade significant sums in taxation, may be attributable to a plethora of factors.[222] Regardless, this case study reveals that it took five years for the FCA to become aware of allegations of criminality, again demonstrating inherent flaws in the UK's ability to ensure the exchange of information between LEAs to

with Respect to Taxes on Income and on Capital Gains with Protocol (Signed June 19 2008, entered into force December 18 2009) 2011 UKTS 005, Art.27(2).
[215] OECD (n 39) para 12.3.
[216] ibid.
[217] J Garside *et al*, 'France Says It Did Not Restrict UK From Using HSBC Files To Pursue Bank and Criminals' The Guardian (February 13 2015) <https://www.theguardian.com/business/2015/feb/13/france-says-it-did-not-restrict-uk-from-using-hsbc-files-to-pursue-bank-and-criminals> accessed March 4 2023.
[218] Treasury Committee, *Oral Evidence: Financial Conduct Authority* (February 10 2015, HC 2014-15, 1055) Q75 and 76.
[219] HM Revenue & Customs, 'HMRC Confirms HSBC Suisse Bank Data Can Now Be Shared' (February 25 2015) <https://www.gov.uk/government/news/hmrc-confirms-hsbc-suisse-bank-data-can-now-be-shared> accessed March 4 2023.
[220] ibid.
[221] First reported by M Kleinman, 'FCA Ends Probe Into HSBC Swiss Tax Affair' Sky News (January 4 2016) <https://news.sky.com/story/fca-ends-probe-into-hsbc-swiss-tax-affair-10334024> accessed March 4 2023.
[222] See J Fisher, 'HSBC, Tax Evasion and Criminal Prosecution' (2015) 1253 Tax Journal 6.

detect and address financial crimes. Unlike in the preceding case studies, the exchange of this information by HMRC would not have prevented money laundering from taking place, but it could have enabled action to be taken in response to this corporate economic crime by appropriate LEAs.

Therefore, despite an extensive legislative framework, HMRC are failing to exchange information with other LEAs in respect of a plethora of financial crimes, including terrorism financing and money laundering. Accordingly, the following section makes important recommendations for reform.

Recommendations

First, minor amendments could be made to the legal framework to improve the exchange of information in tax cases, between HMRC and other LEAs. In this respect, the CRCA 2005 should be amended to require, rather than permit, disclosure when HMRC employees suspect, or have reasonable grounds to suspect, that they are in possession of information that reveals indications of money laundering or terrorism. This would be similar to the obligation to report SARs under the POCA 2002 and TACT. This amendment would emphasise to employees of HMRC that, despite its importance, taxpayer confidentiality should not act as a barrier to information exchange in cases of serious crime and terrorism. In turn, the amendment would provide essential financial intelligence to LEAs, helping to initiate or support investigations into money laundering and preventing terrorist attacks. Second, alternatively or in addition to amendment of s.18, information exchange would be facilitated by the incorporation of an additional statutory function for HMRC in s.5 of the CRCA. To accompany HMRC's primary function of revenue collection, HMRC should be tasked with a subsidiary function of preventing and detecting tax crimes and other financial crimes encountered in the course of its

primary revenue collection function. This would not only help to counteract the culture of secrecy inhibiting information exchange in these important limited circumstances, but also, would help to incentivise HMRC to take a more principled approach to their enforcement activities than the current revenue-collection centred approach.[223] Moreover, a crime prevention function should also encourage HMRC to proactively negotiate wider use of information received under international taxation agreements, enabling dissemination of important intelligence to other LEAs. While simple, these amendments would likely have a profound effect on the UK's ability to combat complex financial crimes, by forcing the UK's tax authority to exchange information and thus, take a more active role in financial crime investigation and enforcement.

Conclusion

This paper addressed the omission in existing literature by providing a uniquely comprehensive examination of the UK's legal framework pertaining to information exchange in terrorism financing and tax evasion investigations. By providing two novel case studies, as well as a holistic examination of national exchange of information provisions, this paper revealed previously undiscovered inadequacies in the existing legal framework relating to financial intelligence and its dissemination. Accordingly, despite favourable evaluations of the UK legal framework by both the FATF and the OECD, this paper demonstrates that the UK is not compliant with international standards concerning financial intelligence and the exchange of information. Thus, the conclusions and findings of the 2018 MER can be questioned. In order to remedy this non-compliance, this paper made a series of timely recommendations for reform. This includes amending the Fraud Act 2006 to introduce an obligation to report fraud for the

[223] See, R de la Feria 'Tax Fraud and Selective Law Enforcement' (2020) 47(2) Journal of Law and Society 240.

regulated sector, thus adopting the same model as money laundering and terrorism financing. In order to address concerns raised by the regulated sector about the potential impact of mandatory reporting on already existing high levels of compliance costs, the paper suggests that these could be partially supported by using funds from the Economic Crime Levy, the Economic Crime Fighting Fund and the redistribution of financial crime related financial penalties imposed by the FCA. Furthermore, the paper recommends that the membership of JMLIT should be extended to include more professional bodies and a wider range of members from the regulated sector. This would encourage and facilitate the voluntary exchange of information where reporting entities are not subjected to civil and/or criminal penalties for non-reporting. HEIs should also become part of the regulated sector for the purposes of AML/CTF legislation. Amongst other preventative measures, this would explicitly task HEIs with an obligation to submit SARs, providing valuable financial intelligence to initiate or support terrorism financing investigations. The paper has also made a series of recommendations to reform the CRCA 2005, which includes 'requiring' HMRC to disclose rather than 'permit' disclosure where HMRC employees suspect they are in in possession of information that reveals money laundering or terrorism. Finally, the paper recommends that the exchange of information would be supported by providing HMRC with a subsidiary function of preventing and detecting tax crimes and other financial crimes alongside its primary revenue collection function.