Exchange of Information and Financial Crime in the United Kingdom

Dr Sam Bourton[1],
Professor Nic Ryder[2]
and Dr Fiona
Brimblecombe[3]

Commissioned by SYNALOGiK

Foreword

Can I share data with my colleagues? Can I share data with other agencies or organisations?

The ability to legally share personal data with and between government departments, law enforcement bodies and third parties in England and Wales is a complex issue. Public sector clients has asked these questions of Synalogik many times. In response, Synalogik Innovative Solutions commissioned a study from the UK's leading academics in this field to address these challenges.

Part 1: Sharing personal data with law enforcement bodies, between law enforcement bodies and in the context of criminal/civil investigations – examines If, how, and when such data can be shared, and how the key principles of the GPDR and the Data Protection Act 2018 do not prohibit personal data being shared with 'competent authorities' performing their 'statutory duty' in law enforcement functions.

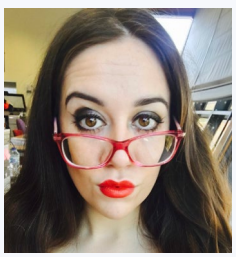
Part 2: The four case studies demonstrate the importance of financial intelligence and information exchange in combatting financial crimes. The case studies illustrate that, in practice, there are inherent flaws in the UK's ability to obtain and exchange information to detect and address these financial crimes. Accordingly, this paper questions the findings of the FATF MER that apply to financial intelligence and the exchange of information and suggests that the UK does not satisfactorily comply with international standards.

Part 3: Discusses the most important and traditional AML/CTF countermeasures are the use of financial intelligence and the impact POCA, TACT, SARS and JMLIT have on Financial Terrorism. The large-scale instances of fraud and the increase in the amount of fraud demonstrates that the UK counter fraud strategy is failing are described with examples, and how financial intelligence is essential in combatting tax evasion.

Authors

[1] Dr. Sam Bourton is a lecturer in Law, Financial Crime and Regulation at Bristol Law School, University of the West of England.

[2] Nic Ryder is a Professor in Financial Crime, School of Law and Politics, Cardiff University.



[3] Dr. Fiona Brimblecombe is a lecturer in Law, Manchester University.

Part 1

Sharing personal data with law enforcement bodies, between law enforcement bodies and in the context of criminal/civil investigations

SYNALOGiK

Introduction

The ability to legally share personal data with and between government departments, law enforcement bodies and third parties in England and Wales is a complex issue. If, how, and when such data can be shared is a pertinent question for law enforcement officials and private companies, and matters are becoming more rather than less convoluted. The UK GDPR is at the forefront of the public conscience, and the UK's protection for privacy rights is currently facing intense media scrutiny under a Conservative government that openly priorities fluidity of business and freedom of expression over personality interests.[4] Helpfully, the ICO [5] has offered guidance as to sharing personal data with law enforcement agencies. 'Personal data' is famously defined broadly in Article 4(1) GDPR:

'...any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person...' [6]

Recital 26 of the Regulation elaborates upon the definition of an identifiable natural person:

'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.[7]

These definitions are very similar to those contained within the EU's previous data protection legal instrument, the 1995 Data Protection Directive, as Article 2(a) of the Directive previously referred to personal data as relating to an 'identifiable natural person' and that account should be taken of the likely means used to identify an individual. [8]

The question of what information can be shared is one of fact and degree: key principles to abide by are necessity, proportionality, and justifications. The UK GDPR and the Data Protection Act 2018 do not prohibit personal data being shared with 'competent authorities' performing their 'statutory duty' in law enforcement functions.[9] Relevant competent authorities include the police, courts, prisons, and government departments.[10] According to s.31 of the DPA 2018, 'law enforcement purposes' includes the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties'.[11] There are caveats to this information sharing. As the Information Commissioner notes, even if a body wishes to share personal data with a law enforcement authority, then a lawful basis needs to be articulated under Article 6(1) GDPR.[12] These include (but are not limited to):

a) Consent: this is unlikely to be obtained during an investigation;
b) Necessary for performance of contract for a data subject: this is unlikely to be relevant;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; this could potentially be relevant to an investigation;
e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; this seems undoubtedly relevant to information shared during criminal/civil investigations – sharing personal data with a view to combat crime could fall within the ambit of public interest (for example if there were reasonable grounds to suspect someone, even if it turned out to be false).[13]

Matters become yet more complicated when the personal data shared is 'special category data.' In its drafting, the GDPR differentiates between different types of personal data: that which is sensitive personal data, otherwise known as 'special category data' and that which is not. In its introduction, the Regulation states that 'sensitive personal data' by way of definition is:

'Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms...'[14]

Special category data includes that which relates to:

- Racial/ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union membership
- Genetic/biometric data that uniquely identifies a person
- Health data
- Data about sex life/sexual orientation.[15]

Special category data is deemed by the GDPR as inherently more personal in nature and therefore further safeguards are present in the legislation relating to its processing. To share personal data in one of these categories ('special category data') with law enforcement authorities, a legitimate ground for processing according to Article 9(2) GDPR needs to apply. The list is lengthy and will not be reproduced here in full, however, the most likely relevant grounds from the perspective of criminal or civil investigations seems to be that in Article 9(2)(g):

'processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'[16]

The definition of a 'substantial public interest' is not articulated in the UK GDPR or the DPA 2018.[17] An argument will have to be made and logged at the time of sharing, lest the disclosure come under scrutiny later in time. Media lawyers will not find this lack of definitional certainty surprising – aside from the well-trod examples of the public interest encompassing, for example, corruption in public office or misuse of funds,[18] the public interest has long been an ephemeral notion assessed on a case-by-case basis, in both common law privacy actions (misuse of private information) and judgments of the European Court of Human Rights under Article 10 ECHR.[19]

The ICO explains that if an organisation wishes to disclose 'criminal offence data'[20] then a lawful basis in Article 6(1) GDPR is once again needed; further, the discloser must be an 'official authority' or a separate condition for processing is required under Article 10 of the UK GDPR.[21] The text of Article 10 is circular, and the DPA 2018 details more specific conditions in Schedule 1. Schedule 1, para 10 dictates:

10(1)This condition is met if the processing—

(a) is necessary for the purposes of the prevention or detection of an unlawful act,
(b)must be carried out without the consent of the data subject so as not to prejudice those purposes, and
(c)is necessary for reasons of substantial public interest.

(2)If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).

(3)In this paragraph—
• "act" includes a failure to act;
• "competent authority" has the same meaning as in Part 3 of this Act (see section 30).'[22]

This need for a further applicable condition in schedule 1 is also relevant for the sharing of special category data. The result of these intertwining sections is that, when sharing criminal offence data, this can lawfully be done if there is a lawful basis for processing under Article 6 UK GDPR, plus Article 10 UK GDPR is satisfied and schedule 1, para 10 of the Data Protection Act 2018.

Schedule 2, para. 2 of the DPA 2018 exempts the transparency principle and individual rights when crime is being detected – if adhering to such principles would compromise an investigation.[23] ICO should be commended for its comprehensive and clear guidance in this regard: it has gone so far as to produce a 'tool' for organisations and business owners that will help navigate whether they should or are able to share data with law enforcement authorities.[24]
Schedule 2 para. 2 of the DPA 2018 contains a Crime and Taxation Exemption:

'Crime and taxation: general

2(1)The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes—

(a)the prevention or detection of crime,
(b)the apprehension or prosecution of offenders, or
(c)the assessment or collection of a tax or duty or an imposition of a similar nature, to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).

(2)Sub-paragraph (3) applies where—

(a)personal data is processed by a person ("Controller 1") for any of the purposes mentioned in sub-paragraph (1)(a) to (c), and
(b)another person ("Controller 2") obtains the data from Controller 1 for the purpose of discharging statutory functions and processes it for the purpose of discharging statutory functions.

(3)Controller 2 is exempt from the obligations in the following provisions of the GDPR—

(a)Article 13(1) to (3) (personal data collected from data subject: information to be provided),

(b)Article 14(1) to (4) (personal data collected other than from data subject: information to be provided),

(c)Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers), and

(d)Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in paragraphs (a) to (c),

to the same extent that Controller 1 is exempt from those obligations by virtue of sub-paragraph (1).'[25]

As can be seen from the text above, this exempts a body sharing personal data with a competent authority from UK GDPR provisions on individual data protection rights, such as the right to be notified of data breaches and 'the right to be informed'.[26] Although this is a wide-ranging exemption in terms of the lengthy list of Articles it bars from operation, it is not necessarily easy to rely on in terms of catchment. A person or body seeking to rely on it must prove a 'direct causal link' between compliance with (exempted) data protection provision and the prevention or detection of crime, if one were arguing the exemption on the grounds of 2(1)(a).[27] The prejudice that complying with the data protection principles one is seeking to exempt must be 'real and substantial'.[28] This is a high threshold – when seeking to rely on this exemption, it would be wise for a body to detail arguments and evidence as to why it is necessary the exemption apply, and why it is proportionate and necessary to exempt such data protection principles from operation.

The ICO notes that the same rules apply to information sharing between non-law enforcement authorities and law enforcement authorities as well as information sharing between different law enforcement agencies under the DPA. In other words, rules are the same between horizontal information sharing between two different law enforcement bodies, and a lay company and a law enforcement

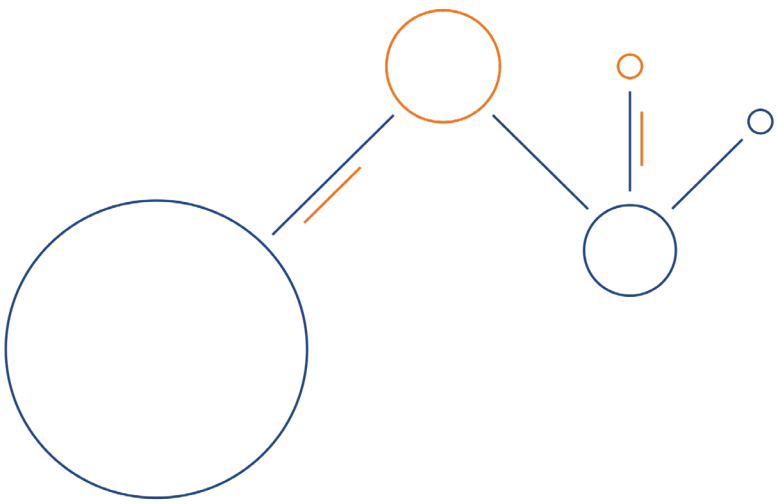
agency.[29] In terms of fighting white collar crime, the UK GDPR does not constitute an absolute bar between law enforcement authorities sharing personal data with each other, for example for the prevention or detection of crime. An organisation must have a lawful basis to share personal data (under Article 6 UK GDPR), and a further condition for processing is necessary for special category data or criminal offence data, which is deemed peculiarly sensitive and therefore a higher threshold is needed in justifications for sharing.[30]

It is important to note that the processing of personal data for 'law enforcement purposes' is covered by the Law Enforcement Directive.[31] With regards to police forces sharing information between one another, the College of Policing has offered constructive training for forces - sharing information 'must be linked to a policing purpose' such as protecting life or preserving order.[32] Agreements to share information between forces can be put into place, such as a 'data processing contract' – where information is shared as processing has been contracted to a third party, or an 'Information Sharing Agreement'('ISA').[33] Training guidelines stress that police do not have 'carte blanche' to share what information they please, even in (what they perceive to be) the interests of fighting crime – College of Policing training shows that an emphasis is placed on considered, thoughtful and purposeful data sharing.[34] The guidance police are receiving is broad in reach; it notes the importance of statutory privacy regimes such as the UK GDPR and the DPA as well as the Human Rights Act 1998 (through which Article 8 ECHR feels impact).[35] Misuse of private information as a common law mechanism may also have relevance to the disclosure of private information – although the interests of fighting crime would likely weigh as an important counter-balance to the ultimate balancing exercise between privacy and competing rights that judges conduct in the second stage of the tort's assessment.[36]

Statutory obligations can also mean that police officers must share information, such as those in the Freedom of Information Act 2000.[37] The guidance for officers shows an awareness that police are often under pressure during fast-paced investigations as to whether to divulge personal data. Regardless of this, the DPA applies; however, the crime and taxation exemption above is often relevant. It is crucial is that an information trail is recorded, of what was shared, to whom and why – and the relevant policing purpose.[38]

In relation to civil claims in particular, the Civil Procedure Rules (the 'white book') details regulations around the disclosure of documents in civil claims, which are lengthy.[39] Multinational law firm Allen & Overy have noted that 'virtually all evidence' a regulator handles when conducting a civil investigation will involve personal data, and there may be need to disclose to third parties because of an obligation.[40] They note that in English, civil litigation, the biggest 'risk' in terms of data protection is disclosing data that is not relevant – it is always possible to redact information in legal proceedings, although this 'is both difficult and costly'.[41] The GDPR raises tensions with companies 'stuck between a rock and a hard place' with disclosure in civil matters: particularly when US law enforcement authorities are involved.[42] GDPR fines against companies are significant,[43] but only have 'teeth' if a company is in a jurisdiction that recognises the GDPR and enforces it. Data subject access requests[44] can also be demanded by data subjects from controllers, to ascertain whether personal data has been processed or given to other organisations; such access requests are not always awarded, and the Exemption in schedule 2 of the DPA may also be relevant to these requests.

Finally, an important caveat is that the UK is currently in a state of flux with regards to data rights. After Brexit, as many academics and practitioners expected, the Conservative Government have announced two reforms that will impact data protection and privacy law and policy: the Data Reform Bill, which will have the ultimate effect of reducing obligations and safeguards present in the UK GDPR, and the Bill of Rights,[45] which will re-centre the privacy-speech debate firmly on the importance of expression, which will have an impact on common law privacy rights. An already complex picture looks likely to become yet more complicated.



Part Two

Four Case Studies on the Exchange of Information in the UK

SYNALOGiK

Case Study 1

Money Laundering: Financial Intelligence and the Exchange of

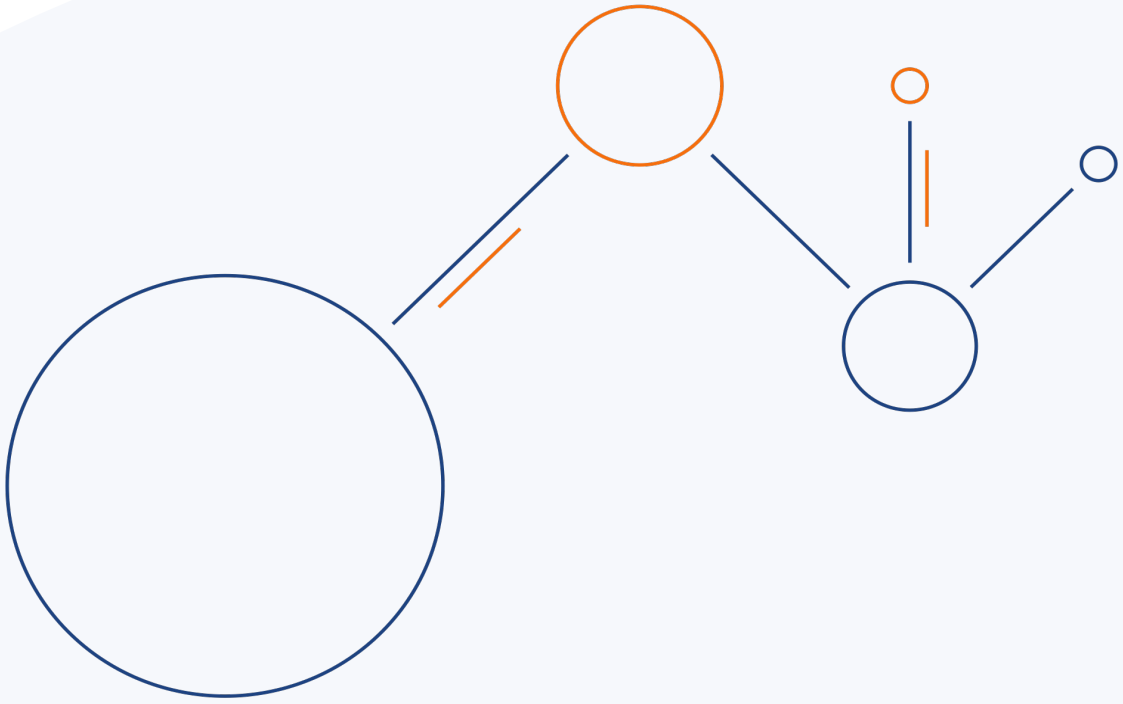
The first line of defence against money laundering are SARs [46], which are submitted to the National Crime Agency (NCA), by reporting entities by virtue of the AML/CTF reporting obligations under the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TACT). Regrettably, the current complicated manual-driven SAR system is considered deficient by all stakeholders, from report authors through to security investigators/analysts, especially owing to its serious absence of rapid triage (classification of urgency/risk/threat levels), dissemination, evidential gathering processes and the inability to cope with the large volumes of SARs.

SARs are under-utilised by LEAs, and LEAs continue to have poor management information on how the reports are used. [47] Notwithstanding these criticisms, the existence of these reporting requirements has created a fear factor across the regulated sector, which in turn has prompted a significant increase in the number of SARs submitted to the NCA. [48] For instance, the number of SARs submitted between 1995 and 2002 increased from 5,000 to 60,000, [49] and the trend remained upwards in subsequent years, as the table below demonstrates:

Year	Number of SARs
April 2009–March 2010	240,582[50]
April 2010–March 2011	247,601[51]
April 2011–March 2012	278,665[52]
April 2012–March 2013	316,527[53]
April 2013–March 2014	354,186[54]
April 2014–March 2015	381,882[55]
April 2015–March 2016	634,113[56]
April 2016–March 2017	463,938[57]
April 2018–March 2019	478,437[58]
April 2019–March 2020	573,085[59]

These increases are directly attributable to the threat of sanctions by organisations such as the FCA.[60] For example, Deutsche Bank AG was fined £163million for failing to maintain adequate AML controls.[61] Here, the FCA concluded that there were serious weaknesses Deutsche Bank's AML controls that included inadequate customer due diligence and deficient AML policies/procedures. Because of these deficiencies, Deutsche Bank, "was used by unidentified customers to transfer approximately $10billion, of unknown origin, from Russia to offshore bank accounts in a manner that is highly suggestive of financial crime".[62] In December 2021, HSBC Plc was fined £63.9million for a series of deficiencies in its AML monitoring and reporting system.[63] HSBC used an automated process to scrutinise millions of transactions to detect money laundering. However, the FCA concluded that there were significant weaknesses in the transaction monitoring systems. The weaknesses

in the relationship between financial intelligence and exchange of information is illustrated by *R v NatWest Bank Plc*.[64] Here, NatWest was charged with failing to adequately monitor the activity of one of its commercial customers, Fowler Oldfield, between 2012 and 2015. During this period, the bank (which had originally indicated it would not take any cash deposits from the customer) accepted £365 million in deposits, of which £264 million was in cash.[65] The banks employees who were responsible for accepting the cash deposits from Fowler Oldfield reported their suspicions to the staff who were responsible for investigating allegations of money laundering. Over 20 internal suspicious reports were raised, yet no SAR was submitted to the NCA. Additionally, the banks automated transaction monitoring system "incorrectly recognised some cash deposits as cheque deposits".[66] NatWest became the first bank to be convicted for failing to comply with the Money Laundering Regulations and was fined £264.7 million.[67]



Case Study 2

Terrorism Financing

This case study questions the findings of the Financial Action Task Force 2018 Mutual Evaluation Report MER [68] and presents evidence that illustrates fundamental weaknesses in the exchange of information between LEAs and the UK Security Services (SIS). [69] In 2003, HMRC connected several instances of fraud with Shahzad Tanweer, one of the July 2005 terrorists, yet the information was not disclosed to LEAs or the SIS. [70] The group linked to Tanweer gained approximately £8 billion from VAT and benefit frauds, of which it sent "1% of its gains, or £80 million, to al-Qaeda in Pakistan and Afghanistan, where it funded madrasahs, training camps and other terrorist activities". [71] It was reported "senior HMRC officials declined to use their intelligence to mount prosecutions and neutralise the gang ... [tax officials] were prevented from sharing intelligence with MI5 due to HMRC's desire to keep tax records confidential". [72]

There are a number of mechanisms that facilitate the exchange of information between HMRC, SIS and LEAs. The reluctance of HMRC to exchange the information contradicts section 19 of the Anti-terrorism, Crime and Security Act 2001, HMRC Information Disclosure 19 Guide (IDG50140) [73] and the Counter Terrorism Act 2008. [74]

The problem is not with the legislation or guidance, but the restrictive interpretation of 'taxpayer confidentiality', which limits the ability of HMRC to exchange information. HMRC practice is not in line with national, regional and international legal instruments. FATF Recommendation 31 provides that "when conducting [terrorist financing] investigations ... competent authorities should be able to obtain access to all [author's emphasis] necessary documents and information for use in those investigations, and in prosecutions and related actions".[75] 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".[76] The reluctance of HMRC to exchange the information with SIS contradicts section 19 of the Anti-terrorism, Crime and Security Act 2001. This section permits the disclosure of information held by 'Revenue Departments' and provides that:

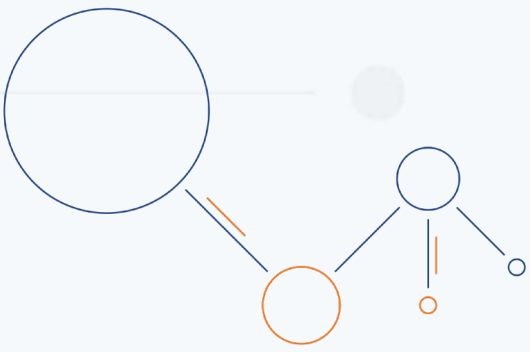
"no obligation of secrecy ... prevents the voluntary disclosure of information ... to assist any [authors emphasis] criminal investigation ... the section allows for disclosure to the intelligence services (the Security Service, the Secret Intelligence Service and GCHQ) in support of their functions. These functions include the protection of national security and the prevention and detection of serious crime".[77]

The disclosure of information with SIS is also permitted by the HMRC Information Disclosure 19 Guide (IDG50140).[78] However, the ability of HMRC to disclose information is restricted by the CRCA 2005, which provides that information must not be disclosed to anyone unless the person making the disclosure has the authority to do so.[79] This applies to HMRC providing information to government departments, LEAs and other public bodies. However, this restriction does not apply if the disclosure is "made for the purposes of a criminal investigation or criminal proceedings (whether or not within the United Kingdom) relating to a matter in respect of which the Revenue and Customs have functions".[80]

HMRC's duty of confidentiality is also "subject to any other enactment permitting disclosure",[81] 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".[82] The functions of the SIS are:

"the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means ... [and] to safeguard the economic well-being of the United Kingdom".[83]

Interestingly, HMRC also has a 'duty to co-operate' and 'disclosure' under the 2017 Money Laundering Regulations.[84] The Regulations provide that "co-operation may include the sharing of information [author's emphasis] which the supervisory authority is not prevented from disclosing".[85] The case study questions the decision not to disclose the information to SIS for there are a number of mechanisms that facilitate the exchange of information between HMRC, SIS and related LEAs. The problem is not with the legislation or guidance, but the restrictive interpretation of 'taxpayer confidentiality', which limits the ability of HMRC to exchange information. Interestingly, this is not the first time that HMRC has been criticised for non-disclosing information, as demonstrated by the following case study. Therefore, in light of these findings, it appears that the HMRC practice is not in line with national, regional and international legal instruments. The evidence presented in this section illustrates that UK has not met the information exchange requirements of the FATF Recommendations.



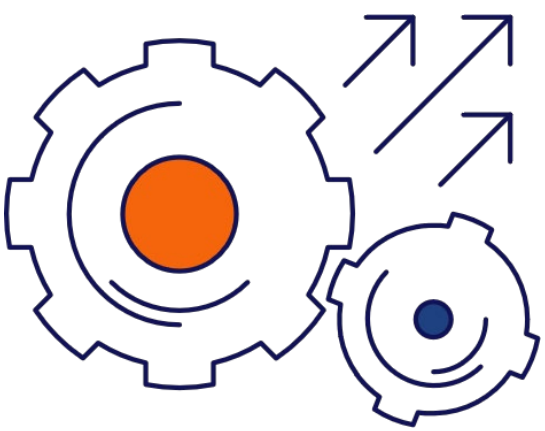
Case Study 3 – Tax Evasion

This case study builds on the findings of the second case study and presents further findings that illustrate weaknesses within tax fraud, financial intelligence and the exchange of information. 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 Private Bank (Suisse) had assisted numerous wealthy clients to evade paying millions of pounds in tax.[86] The International Consortium of Investigative Journalists reported that HSBC (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, including former and

current politicians, 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; the whistle blower, Herve Falciani, reported that not only had HSBC set up these accounts, but also, reassured its international clients that details of accounts held would not be disclosed to national authorities, regardless of indications of undeclared assets.[87] In fact, HSBC wrote to its customers to inform them how to get around the application of the European Savings Tax Directive, designed to counter tax evasion, and provided individuals with anonymous credit cards to withdraw funds without detection.[88] 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.[89] HMRC's response to the HSBC scandal has been seen as disappointing and even "seriously legally flawed".[90] 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.[91] Despite HMRC's claims to the contrary, this is in sharp contrast to action taken in other jurisdictions, such as France and the United States, both of which reached a Deferred Prosecution Agreement with, and imposed significant penalties on, HSBC (Suisse).[92] When appearing before the Public Accounts Committee, 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.[93] 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 (including courts and administrative bodies) 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, or the oversight of the above. Such persons or authorities

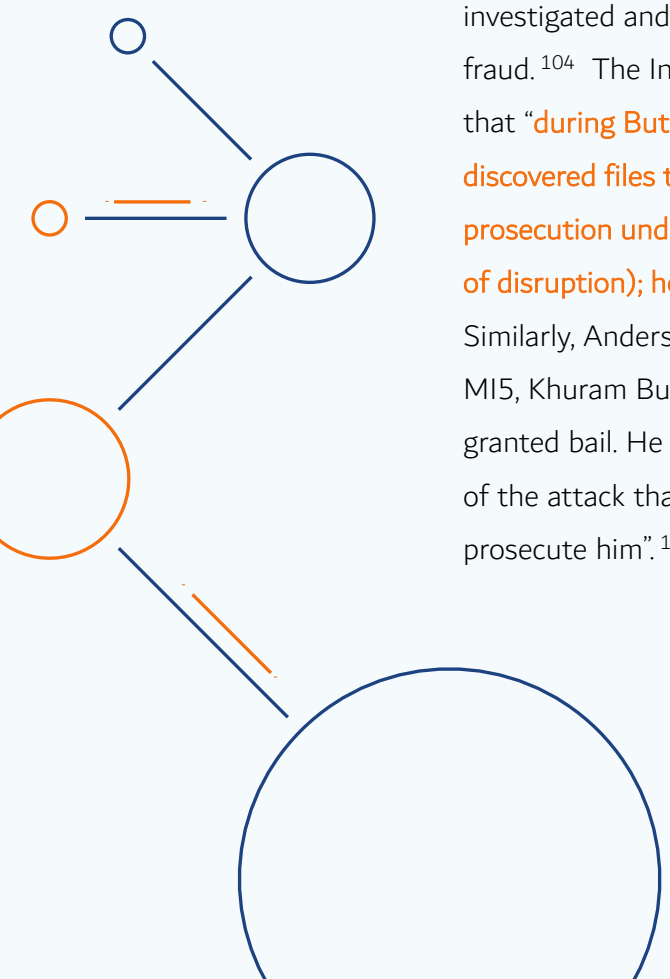
shall use the information only for such purposes". [94] However, the UK-France Treaty is modelled on the OECD's Tax Convention on Income and on Capital, which provides that the Convention "allows the sharing of tax information by the tax authorities of the receiving State with other LEAs and judicial authorities in that State on certain high priority matters (e.g. to combat money laundering, corruption, terrorism financing)". [95] Accordingly, information can be exchanged with other LEAs in accordance with the Convention when two conditions are met: specifically, the laws of both countries must permit the use of the information for other purposes and the supplying state must authorise such use. [96] HMRC claimed that it asked the French authorities for permission to share the data with other LEAs in 2010; a claim that was disputed at the time by France's Finance Minister. [97] In any event, the activities of HSBC (Suisse) were only revealed to the Financial Conduct Authority (FCA) and other LEAs in 2015, following the dissemination of the information in the media. [98] Following this, on 23 February 2015, 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. [99] HMRC later met with LEAs including the Serious Fraud Office (SFO), the NCA and the FCA to consider sharing of the data.[100] However, all investigative activities were discontinued within 12 months. [101]

The UK's ultimate failure to act against a UK-headquartered bank, which assisted clients around the world to evade significant sums in taxation, may be attributable to a plethora of factors. [102] Nevertheless, this case study reveals that it took five years for the UK's financial services industry regulator to even become aware of allegations of criminality on behalf of a major British bank, again demonstrating inherent flaws in the UK's ability to ensure the exchange of information between LEAs to detect and address financial crimes.



Case Study 4 Fraud

The final case study illustrates the link between fraud and other serious crimes, as well as further weaknesses inherent in the UK's approach to obtaining and exchanging financial intelligence. In June 2017, eight people were killed by terrorists who drove a van into pedestrians on London Bridge before a knife attack in Borough Market.[103] One of the terrorists, Khuram Butt, was investigated and arrested in October 2016 for a suspected fraud.[104] 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 Terrorism Act' (offering a further means of disruption); however ... the issue was not explored further".[105] 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".[106] 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 (against Butt) could be taken, due to a lack of evidence".[107] It is important to note here that Santander, was under no legal obligation to report the alleged fraud committed by Butt.

The Fraud Review noted that "fraud is massively underreported".[108] Fraud is not a police priority, so even when reports are taken, little is done with them. Many victims, therefore, don't report at all. The official crime statistics display just the tip of the iceberg and developing a strategic LEA response is impossible because the information to target investigations does not exist.[109] If a suspected fraud is committed a reporting entity must report such to its Money Laundering Reporting Officer (MLRO). Successful frauds are then reported to the NCA. The obligation to report allegations of fraud is not, however, straightforward. The primary statutory obligation for reporting instances of fraud is contained under the POCA 2002.[110] It is a criminal offence under the Act to fail to disclose via a SAR where there is knowledge, suspicion or reasonable grounds to know or suspect, that a person is laundering the proceeds of criminal conduct. Successful fraud is defined as money laundering for the purpose of this Act.[111] Furthermore, the Act specifies that members of the regulated sector are required to report their suspicions as soon as reasonably practical to the NCA via their MLRO. However, there is no legal obligation to report unsuccessful or attempted frauds to the authorities because any attempted frauds will not give rise to any legal criminal proceedings and therefore fall outside the scope of the mandatory reporting obligations. Ultimately, the decision whether or not an investigation will be conducted lies with the police. The Home Office has advised that the police should only investigate where there are good grounds to believe that a criminal offence has been committed.[112]

In order to address this deficiency, the Fraud Review,[113] recommend that businesses and individuals could report fraud to the National Fraud Reporting Centre (NFRC). This recommendation resulted in the creation of the National Fraud Intelligence Bureau (NFIB), an agency dedicated to analysing and assessing fraud with the aid of

analysts from both LEAs and the private sector.[114] The NFIB was managed by the City of London Police as part of its role as the National Lead Force for fraud and was funded by the Home Office. The NFRC "became established as Action Fraud run by the City of London Police".[115] These measures are "an impressive list of strategic aims: tackling the key threats of fraud that pose the greatest harm to the UK".[116] However, Action Fraud was abolished following a 2019 investigation by The Times which illustrated how Action Fraud's staff were trained to mislead victims of fraud that their cases were actually being investigated.[117] According to The Times, less than two percent of reports submitted to Action Fraud resulted in an arrest and less than one percent of police officers were assigned to fraud investigations. Consequently, the Home Office commissioned a review of how fraud is policed in the UK by Sir Craig Mackey, which agreed with the findings of The Times and concluded that the police are not adequately prepared to tackle fraud.[118] As a result, HMG announced in July 2021 that Action Fraud was to be abolished and placed within the NCA.[119] [120] The decision to place fraud within the NCA is questionable because it has been described as "incompetent" and "negligent" after its mistakes resulted in the collapse of a fraud trial in 2014.[121] Furthermore, the NCA were criticised for failing to investigate reports relating to banks forged signatures in court action to repossess properties.[122] HMICFRS concluded that the NCA "does not have dedicated fraud investigation teams but will allocate resources to investigate complex frauds on a case-by-case basis".[123]

Conclusion

The four case studies demonstrate the importance of financial intelligence and information exchange in combatting financial crimes. The case studies illustrate that, in practice, there are inherent flaws in the UK's ability to obtain and exchange information to detect and address these financial crimes. Accordingly, this paper questions the findings of the FATF MER that apply to financial intelligence and the exchange of information and suggests that the UK does not satisfactorily comply with international standards.

Part 3

Financial Terrorism

SYNALOGiK

Money Laundering and Terrorism Financing

The most important and traditional AML/CTF counter-measures are the use of financial intelligence. The UK introduced its first money laundering reporting requirements by virtue of the Drug Trafficking Offences Act 1986, which has since been amended by POCA 2002 and the Money Laundering Regulations 2017.[124] A wide range of financial institutions in the regulated sector are thus required to report any allegations of money laundering to the NCA. This includes credit institutions, financial institutions, auditors, insolvency practitioners, external accountants, tax advisors, independent legal professionals, trust or company service providers, estate agents, high-value dealers and casinos. One particularly important regulation is that relevant persons are required to adopt a greater risk-based approach, especially with regard to due diligence. Specifically, the Regulations refer to general risk assessments, risk mitigation policies, increased levels of due diligence, reliance on third parties undertaking customer due diligence and a wider interpretation of what is a "politically exposed person".[125] If a reporting entity suspects that it is being used for the purposes of money laundering, it is required to notify its MLRO, who must then complete a SAR and file it with the NCA, which determines if further action is

necessary. In addition to the use of SARs, the POCA 2002 contains three mechanisms to assist in the exchange of information. For example, a customer information order compels a financial institution to disclose the information it has on the person specified in the application.[126] Additionally, an account monitoring order compels a financial institution to provide specific account information relating to an account or accounts held at a specific financial institution.[127] Finally, a disclosure order requires the recipient to answer questions, provide information and/or produce documents.[128]

TACT makes it a criminal offense to fail to disclose knowledge or suspicion of another person that has committed an offense under the terrorist financing criminal offences.[127] Such a failure to disclose information is identical to the offense of failing to disclose information under the POCA 2002.[130] An individual or organization who suspects that an offense 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".[131] In R v DA Silva, Lord Justice Longmore took the view that

"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'.[132]

Moreover, according to the Court of Appeal in *K v National Westminster Bank*, HMRC, SOCA,[133] 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'.[134] However, the overall effectiveness of this SAR regime has been called into question. As demonstrated by Case Study One, its deficiencies include an ineffective SARs database, weak monitoring of enforcement outcomes, inadequate training and a lack of governmental support.

In addition to the traditional means of gathering financial intelligence via the use of SARs the TACT also 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 investigations".[135] 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".[136] 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".[137] If a financial institution fails to comply with the financial information order it is guilty of a criminal offence.[138] The financial institution, however, does have a defence to breaching the financial information order when they can illustrate that "(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".[139] Additionally, the TACT permits the use of account monitoring orders.[140] 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."[141] 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.[142]

One of the most important developments in financial intelligence, alongside the SARs regime, is the voluntary exchange of information. The FATF has noted, "effective information is one of the cornerstones of a well-functioning CTF framework".[143] 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".[144] 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 to tackle high-end money laundering and other economic threats.[145] According to the FCA, JMLIT has "made very quick progress in aiding voluntary information sharing ... and has quickly demonstrated [its] ... benefits".[146] This has enabled the UK to become a global leader in the exchange of information between

reporting entities and LEAs. For example, the UK model has been adopted in Australia,[147] Singapore[148] and Hong Kong.[149] Indeed, the FATF has concluded that "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".[150]

The exchange of information has also been facilitated by the Criminal Finances Act 2017, which permits 'voluntary disclosures within the regulated sector' as an additional exchange of information mechanism.[151] The Criminal Finances Act 2017 amends both POCA and TACT allowing 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 and/or terrorist financing offence".[152] Furthermore, information sharing can either be instigated by the regulated sector or the NCA.[153]

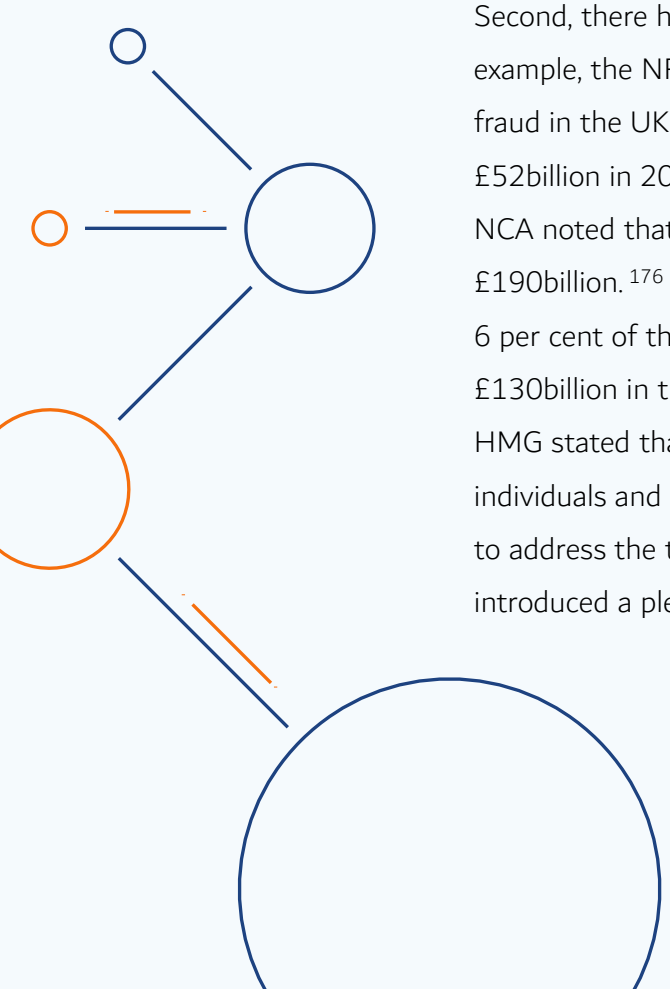
The aim of this statutory provision is to permit reporting entities to share information with each other on a voluntary basis in relation to a suspicion that a person is engaged in money laundering.[154] The provision supports the pre-existing statutory provisions introduced by the Crime and Courts Act 2013, which permits reporting entities to act as information gateways to facilitate the exchange of information between the private sector and LEAs.[155] 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 ... [enabling] it to act as an information intermediary between LEAs and reporting entities'.[156] Information provided via such mechanisms is contained within what are known as 'Super SARs'.[157] Two further information sharing pathways – the Financial Crime Information Network (FIN-NET) and the Shared Intelligence Service (SIS), both of which are hosted by the FCA – enable the sharing of information between LEAs and financial regulatory agencies.[158] It is important to note that all of these mechanisms are voluntary and that a reporting entity is permitted to decline an invitation to exchange information. Of course, information sharing and increased co-operation can result in more comprehensive financial profiles of particular 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 they could provide more useful intelligence if the membership of JMLIT were expanded or if there was greater dissemination of information, particularly regarding emerging trends in money laundering activity.[159]

Another criticism has been that the JMLIT does not engage with reporting entities that are particularly vulnerable to abuse by money launderers. For example, it seemingly focuses exclusively on working with the financial services sector while ignoring other professions, such as accountants,[160] lawyers[161] and estate agents.[162] In 2018, 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'.[163] In response, the NCA stated, 'we do not believe that a simple expansion of the current JMLIT would be the most effective mechanism for wide engagement'.[164] 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 on a short-term basis to allow for their resources/expertise in connection with a particular piece of work'.[165] Although the creation of the JMLIT and the resultant information sharing has achieved some notable successes, it now seems necessary for the UK government to widen the scope of the information sharing model to include social media platforms and other industries.

Fraud

The large-scale instances of fraud and the increase in the amount of fraud demonstrates that the UK counter fraud strategy is failing. There have been egregious instances of fraud – Polly Peck,[166] the Mirror Group Pension Scheme,[167] Guinness,[168] Barlow Clowes,[169] the manipulation of the London Interbank Offered Rate and the Foreign Exchange market[170] and fraud associated with the global pandemic.[171] Second, there has been a significant increase in fraud.[172] For example, the NFA conservatively estimated that the extent of fraud in the UK increased from £30billion in 2010,[173] £52billion in 2011,[174] £73billion in 2013.[175] In 2017, the NCA noted that the amount of fraud had increased to £190billion.[176] Globally fraud losses account for approximately 6 per cent of the global GDP, which totals £3.89trillion, or £130billion in the UK.[177] The most recent figures offered by HMG stated that fraud accounts for 42% of all crime against individuals and costs society £4.7billion per year.[178] Therefore, to address the threat of fraud successive HMGs have introduced a plethora of counter-fraud reporting initiatives.

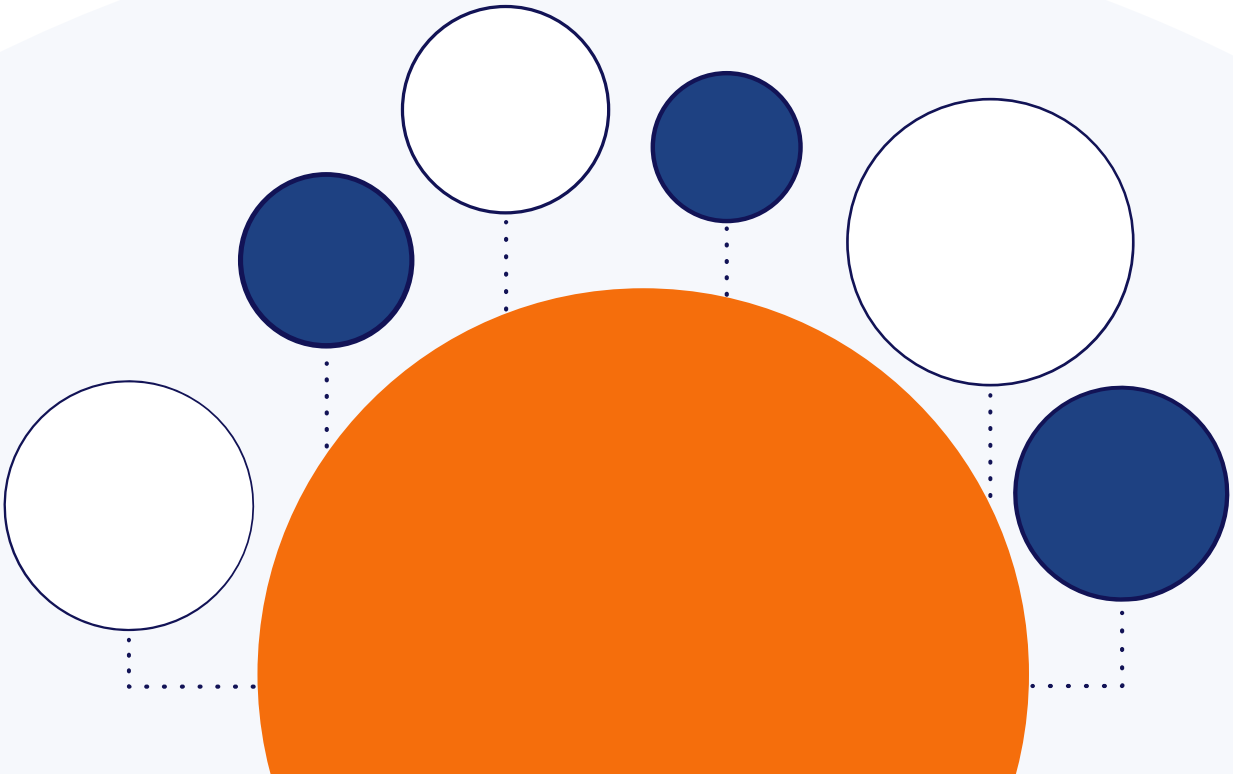


In 2007, the Home Office announced that victims of credit card, cheque and online banking fraud are to report the matter to banks and financial institutions. The obligation to report allegations of fraud is not straightforward, but nonetheless still important. The primary statutory obligation for reported instances of fraud is contained under the POCA 2002. Successful fraud is defined as money laundering for the purpose of this Act. Furthermore, the Act specifies that members of the regulated sector are required to report their suspicions 'as soon as reasonably practical' to the NCA via their MLRO. There is no legal obligation to report unsuccessful or attempted frauds to the authorities because any attempted frauds will not give rise to any legal criminal proceedings that are available for money laundering, and fall outside the scope of the mandatory reporting obligations under the POCA 2002. Ultimately, the decision lies with the police whether or not an investigation will be conducted. The Home Office has advised that the police should only investigate where there are good grounds that they believe a criminal offence has been committed.[179] Given the cuts in the budget for police and the increase in administrative workload for police officers, it is not surprising that the police have not been at the forefront for tackling financial crime.

Members of the regulated sector are obliged to report fraud to the FCA. The FCA Handbook also provides that "the notifications under SUP 15.3.17 R are required as the FCA needs to be aware of the types of fraudulent and irregular activity which are being attempted or undertaken, and to act, if necessary, to prevent effects on consumers or other firms".[180] Therefore, "a notification under SUP 15.7.3 G should provide all relevant and significant details of the incident or suspected incident of which the firm is aware".[181] Furthermore, "if the firm may have suffered significant financial losses as a result of the incident, or may suffer reputational loss, and the FCA will wish to consider this and whether the incident suggests weaknesses in the firm's internal controls".[182] If the institution has suffered a significant financial loss, or may suffer reputational loss as a result of the fraudulent activity, the FCA will take into account whether the incident suggests weaknesses in the institution's internal controls. If the fraud is committed by representatives and other Approved Persons, the FCA has the power to withdraw its authorization and there is the possibility of prosecution.

The Fraud Advisory Panel reported that three quarters of its members felt that mandatory reporting of fraud should be introduced. They sated, "at present there is no legal requirement in the United Kingdom for an organisation to report a fraud to law enforcement should one occur".[183] This is in contrast to money laundering where those reporting in the regulated sector have a duty to prepare a SAR should an offence be suspected".[184]

The Serious Crime Act 2007 permits public authorities to disclose information for the purposes of preventing fraud in accordance with the Specified Anti-Fraud Organisations (SAFOs).[185] "Section 68 of the SCA provides for public authorities to disclose information for the purposes of preventing fraud, or a particular kind of fraud, as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made with such an organisation".[186] An anti-fraud organisation is defined in the Serious Crime Act 2007 as "any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes".[187] There are currently 11 anti-fraud agencies – BAE Systems Applied Intelligence Limited; Callcredit Information Group Limited; CIFAS; Dun and Bradstreet Limited; Equifax Limited; Experian Limited; Insurance Fraud Bureau; Insurance Fraud Investigators Group; N Hunter Limited; Synectics Solutions Limited and Telecommunications United Kingdom Fraud Forum Limited.[188]



Tax Evasion

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 suspected tax evader the opportunity to disclose their fraudulent conduct via a Contractual Disclosure Facility, in exchange for a guarantee that the taxpayer will not face criminal investigation or prosecution.[189] HMRC uses Code of Practice 8 (CoP8) to resolve "cases where the CoP9 is not used".[190] 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.[191] 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."[192]

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.[193] 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',[194] or otherwise under its preserved production powers relating to the type of tax at issue.[195] These powers enable HMRC to request documents from third parties when there are reasonable grounds to suspect tax fraud.[196] The powers are designed to prevent searches of property owned by innocent third parties.[197] HMRC similarly has the power to issue disclosure notices, also aimed at third parties, under the Serious Organised Crime and Police Act 2005.[198] Failing to comply or providing false or misleading information in response to the disclosure notice is a criminal offence.[199] HMRC has the power to apply for search warrants and execute seizures under PACE,[200] and the POCA,[201] 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.[202] Relevant HMRC officers can arrest suspects for indictable tax offences and search property following arrest,[203] but may not charge or bail suspects, or take their fingerprints.[204] At all times, HMRC has access to information that is ordinarily available, including government records and social networking sites.[205] In certain cases, HMRC has the power to employ intrusive surveillance powers.[206]

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.[207] 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.[208] HMRC regularly receives reports from the FIU and is the largest recipient of SAR data.[209] Nevertheless, HMRC has been criticised for not making full use of this intelligence,[210] using only just over one percent of the 300,000 reports it received in 2013.[211] 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.[212] In 2018-19,

SAR data assisted HMRC in recovering £40.2 million through civil enquiries and over £30 million from civil investigations.[213] In 2019-20, these figures declined to £33.5 million and over £15 million respectively.[214]

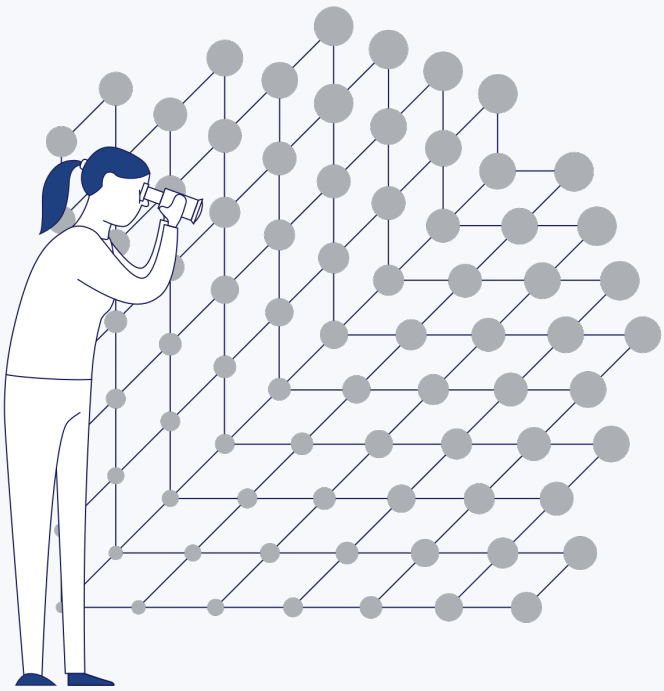
Case Study Four demonstrates HMRC's reluctance to exchange information with national LEAs for the purposes of combatting terrorism financing, allegedly owing to "taxpayer confidentiality".[215] Indeed, the confidentiality of taxpayer information has received both common law and statutory protection since the inception of the income tax,[216] being considered a "vital element in the working of the system" of revenue collection.[217] 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.[218] 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.[219] However, s.18 contains several exceptions to the duty of confidence. For instance, information may be disclosed to pursuant to a function of HMRC.[220] This has been interpreted narrowly by HMRC as not permitting the disclosure of information to Parliamentary committees and inquiries.[221] 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.[222] 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.[223] In regards to disclosure to LEAs, information may also be disclosed to prosecuting authorities,[224] 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.[225] For instance, with consent of the Commissioners, information may be disclosed for the purposes of public safety, or the prevention or detection of crime.[226] However, HMRC note that this exception also applies in "very limited circumstances."[227]

Importantly, HMRC's duty of confidentiality is also "subject to any other enactment permitting disclosure",[228] 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 HMRC to disclose information to LEAs, such as the FCA and the SFO, for criminal investigation purposes.[229] In addition, s.19 of the Counter Terrorism Act 2008 permits disclosure to the intelligence services (MI5, MI6, GCHQ) 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.[230] 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 studies.

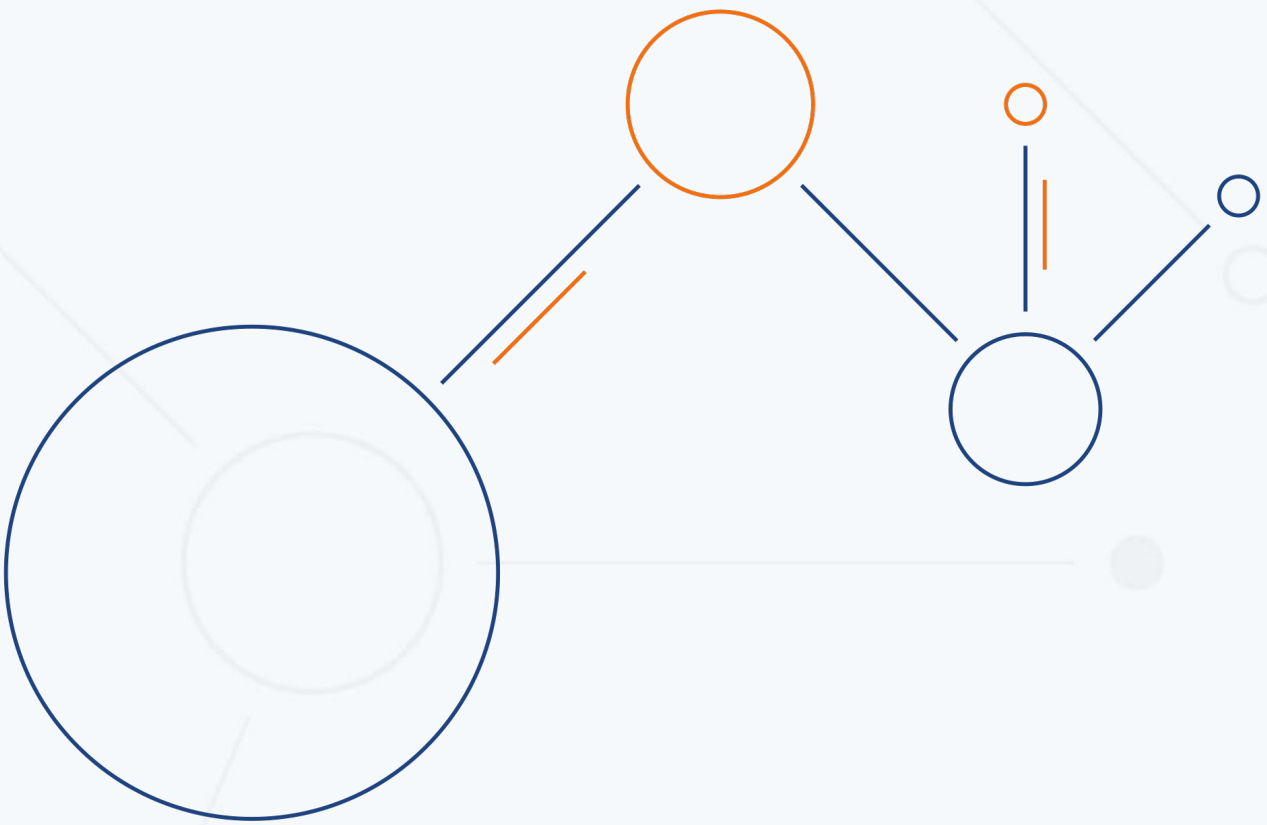
The reason for HMRC's failure to disclose information thus lies not in the absence of a legal gateway, but rather, in HMRC's application of the CRCA. Following an inquiry into HMRC's approach to settling large tax disputes, in written evidence to the Public Accounts Committee, the then Permanent Secretary for Tax at HMRC explained that the CRCA provides "a power, rather than an obligation, to disclose."[231] 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.[232] The issue is exacerbated by HMRC's narrow interpretation of the legislative provisions, often leading to an unwillingness to consent to information disclosure.[233] Moreover, there appears to be limited scope for challenging HMRC's interpretation of the CRCA, with a legal challenge by the PAC previously blocked purportedly due to a lack of funding.[234] 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.[235] 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." [236] Aside from the threat of criminal prosecution, HMRC staff will also be aware of HMRC's prior treatment of whistleblowers, 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 untrue suspicions that he had also disclosed information to the media. [237] 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. [238] 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 professional enablers of these activities. [239] After investigating the Panama Papers leak, JFAC was tasked with leading LEA exploitation of criminal intelligence on financial crime, particularly, bulk financial data. [240] 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. [241] 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." [242] 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." [243] 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 studies above demonstrate 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.



Footnotes

[1]Lecturer in Law, Bristol Law School, University of the West of England, Bristol.

[2] Professor in Financial Crime, School of Law and Politics, Cardiff University.

[3] Lecturer in Law, Manchester University.

[4] See the Government's plans as of June 2022 to introduce a 'Bill of Rights' in order to re-centre the importance of freedom of expression over competing interests, such as privacy/reputation, which has traditionally been given equal footing to expression as a qualified right under Article 8 of the European Convention on Human Rights: https://www.gov.uk/government/news/bill-of-rights-to-strengthen-freedom-of-speech-and-curb-bogus-human-rights-claims.

[5] The Information Commissioner's Office, based in Cheshire, is an independent specialist regulatory body that oversees the implementation of the Data Protection Act 2018 and the GDPR, and advises on privacy, freedom of expression and data rights: https://ico.org.uk/. It is a 'non-departmental' public body.

[6] GDPR, Article 4(1) [emphasis added].

[7] GDPR, Recital 26 [emphasis added].

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of the free movement of such data [1995] O.J L 281, 31 Article 2(a) and Recital 26. Mark J Taylor, 'Data Protection: Too Personal to Protect?' (2006) 3(1) SCRIPT-ed 72, 75 and Paul De Hert and Vagelis Papakonstantinou, 'The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals' (2012) 28(2) Computer Law & Security Review 130,183.

[9] See the Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[10] Data Protection Act 2018, Schedule 7.

[11] Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[12] Ibid.

[13] This is an edited, amended list – text is that of the author's – for full list, see Article 6 GDPR.

[14] GDPR (51).

[15] Article 9(1) GDPR.

[16] Article 9(2)(g) GDPR. Further, the ICO has noted that this would be the relevant justification in such a context: Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[17] Ibid ICO – the ICO is open in its guidance that there is no clear answer here.

[18] See for example: Diane Zimmerman, 'Requiem for a Heavyweight: A farewell to Warren and Brandeis's privacy tort' (1983) 68(2) Cornell Law Review 291, 326 and Von Hannover v Germany (No.2) App nos 40660/08 and 60641/08 (ECHR, 7 February 2012) [102].

[19] For an analysis of misuse of private information jurisprudence in conjunction with the GDPR, see: Fiona Brimblecombe, 'The Public Interest in Deleted Personal Data? The Right to be Forgotten's Freedom of Expression Exceptions Examined through the Lens of Article 10 ECHR' (2020) 23(1) Journal of Internet Law 1-29.

[20] Which is personal data relating to offenders or potential offenders in the context of criminal activity, or alleged criminal activity – including investigations. See further: Further, the ICO has noted that this would be the relevant justification in such a context: Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[21] Ibid ICO.

[22] Ibid ICO, Data Protection Act 2018, emphasis added.

[23] Ibid ICO and see Data Protection Act 2018, Schedule 2, para. 2(1):'The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject) do not apply to personal data processed for any of the following purposes—(a)the prevention or detection of crime,(b)the apprehension or prosecution of offenders, or (c)the assessment or collection of a tax or duty or an imposition of a similar nature,to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).'

[24] Accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[25] Emphasis added.

[26] Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[27] As above.

[28] Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

[29] Ibid and Data Protection Act 2018, Part 3.

[30] Ibid ICO.

[31] Law Enforcement Directive (EU) 2016/680. See College of Policing, 'Information Sharing' accessible at: https://www.college.police.uk/app/information-management/information-sharing and 'Personal Data and Enforcement' Financial Conduct Authority (30/4/21) at: https://www.fca.org.uk/privacy/personal-data-and-enforcement.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Although for how much longer this is relevant remains to be seen – see current reform proposals relating to a Bill of Rights, n.1.

[36] Much has been written on this balancing exercise. See for example: Rebecca Moosavian, 'A just balance or just imbalance? The role of metaphor in misuse of private information' (2015) 7(2) Journal of Media Law 196, 217 and Paul Wragg, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) Journal of Media Law 225.

[37] College of Policing, 'Information Sharing' accessible at: https://www.college.police.uk/app/information-management/information-sharing.

[38] Ibid.

[39] See the Ministry of Justice, 'part 31 - disclosure and inspection of documents' accessible at: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31.

[40] See 'GDPR for litigators' Allen & Overy Blog, accessible at: https://www.allenovery.com/en-gb/global/news-and-insights/publications/gdpr-for-litigators-2019.

[41] Ibid.

[42] Ibid.

[43] For example, failure to comply with Article 5 GDPR, the 'data protection principles' leaves a controller open to the highest tier of administrative fines, according to Article 85(a) GDPR: also see The principles', (The Information Commissioner's Office) accessible at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/.

[44] Ibid.

[45] See fn 1 regarding the Bill of Rights and 'New data laws to boost British business, protect consumers and seize the benefits of Brexit' Department of Digital Culture, Media and Sport and Rt. Hon Nadine Dorries (17 June 2022) at: https://www.gov.uk/government/news/new-data-laws-to-boost-british-business-protect-consumers-and-seize-the-benefits-of-brexit.

[46] Financial Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures United Kingdom Mutual Evaluation Report (2018).

[47] KPMG, Money Laundering: Review of the Reporting System (2003), 14.

[48] R. Sarker, 'Anti-money laundering requirements: too much pain for too little gain' (2006), Company Lawyer, 27(8), 250–251, at 251.

[49] KPMG, Money Laundering: Review of the Reporting System (2003), 14.

[50] Serious Organised Crime Agency, The Suspicious Activity Reports Regime Annual Report 2010 (2010),

[51] Serious Organised Crime Agency, The Suspicious Activity Reports Regime Annual Report 2011 (2011), 10.

[52] Serious Organised Crime Agency, The Suspicious Activity Reports Regime Annual Report 2012 (2012), 12).

[53] National Crime Agency, The Suspicious Activity Reports Regime Annual Report 2013 (2013), 6.

[54] National Crime Agency, The Suspicious Activity Reports Regime Annual Report 2014 (2014), 7.

[55] National Crime Agency, The Suspicious Activity Reports Regime Annual Report 2015 (2015), 7.

[56] National Crime Agency, SARs Annual Report 2017 (2017), 6. (There was no 2015–2016 report.)

[57] National Crime Agency, SARs Annual Report 2018 (2018), 3.

[58] National Crime Agency, SARs Annual Report 2019 (2019), 4.

[59] National Crime Agency, SARs Annual Report 2020 (2020), 4.

[60] A. Leong, 'Chasing dirty money: domestic and international measures against money laundering' (2007), Journal of Money Laundering Control, 10(2), 140–156, at 142.

[61] Financial Conduct Authority 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings', January 1 2017, available from https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure, accessed June 16 2022.

[62] Financial Conduct Authority 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings', January 1 2017, available from https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure, accessed June 16 2022.

[63] Financial Conduct Authority 'FCA fines HSBC Bank plc £63.9 million for deficient transaction monitoring controls', December 17 2021, available from https://www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls, accessed June 6 2022.

[64] Financial Conduct Authority 'NatWest fined £264.8 million for anti-money laundering failures', December 13 2021, available from https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures#:~:text=NatWest%20failed%20to%20comply%20with,money%20laundering%20and%20terrorist%20financing., accessed June 16 2022.

[65] Ibid.

[66] Financial Conduct Authority 'NatWest fined £264.8 million for anti-money laundering failures', December 13 2021, available from https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures#:~:text=NatWest%20failed%20to%20comply%20with,money%20laundering%20and%20terrorist%20financing., accessed June 16 2022.

[67] S.I 2157/2007.

[68] Financial Action Task Force Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report (Financial Action Task Force: Paris, 2018)

[69] The exchange of information between HM Government departments was criticised by the OECD who noted that "the case studies show that it remains a challenge to make sure that interdepartmental contacts exceed the level of fragmented information sharing [in the United Kingdom]". See OECD Whole of Government Approaches to Fragile States (OECD: 2006) at 29.

[70] It has been reported that Shahzad Tanweer left £121,000 in his will, even though he worked on a part-time basis in a fish and chip shop. See Goodchild, S. 'The mystery of the London bomber and his secret wealth', June 8 2006, available from https://www.independent.co.uk/news/uk/crime/the-mystery-of-the-london-bomber-and-his-secret-wealth-522102.html, accessed June 19 2020. It has been suggested that HMRC became aware of the tax fraud scheme as early at 1995. See Mushtaq, W. 'Imran Hussain's father says not responsible for Scottish-Pakistani son's £300m fraud', November 24 2019, available from https://www.geo.tv/latest/258285-imran-hussains-father-says-not-responsible-for-scottish-pakistani-sons-300m-fraud, accessed June 22 2020.

[71]

[72] SE Williams, '£80m of British Taxpayers' Money 'Funnelled to Al-Qaeda' in Decades-Long Scam' (The Telegraph, 31 March 2019) <https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled-al-qaeda-decades-long/> accessed 14th May 2022.

[73] HM Revenue and Customers 'HMRC Internal Manual Information Disclosure Guide', March 19 2016, available from https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg50140, accessed June 19 2020.

[74] Counter Terrorism Act 2008, s. 18(1).

[75] See Financial Action Task Force above, n 2 at 25. A competent authority is defined by the Financial Action Task Force as including "including regulators, tax authorities, FIUs, law enforcement, intelligence authorities, accrediting institutions, and potentially self-regulatory organisations in some jurisdictions". See Financial Action Task Force above, n 2 at 63.

[76] Ibid., at 226.

[77] Anti-terrorism, Crime and Security Act 2001, s. 19.

[78] HM Revenue and Customers 'HMRC Internal Manual Information Disclosure Guide', March 19 2016, available from https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg50140, accessed June 19 2020.

[79] Commissioners for Revenue and Customs Act 2005, s. 18(1). For a more detailed discussion see Mba, O. 'Transparency and accountability of tax administration in the UK: the nature and scope of taxpayer confidentiality' (2012) British Tax Review, 2, 187-225. Also see R v (Ingenious Media Holdings plc) & Anor v HMRC [2016] UKSC 54 and Daly, S. 'R. (Ingenious Media) v HMRC: public disclosures and HMRC's duty of confidentiality' (2017) British Tax Review, 1, 10-21.

[80] Commissioners for Revenue and Customs Act 2005, s. 18(2)(d).

[81] Commissioners for Revenue and Customs Act 2005, s.18(3).

[82] Counter Terrorism Act 2008, s. 18(1).
[83] Security Service Act 1989, s. 1(2) and (3).

[84] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, S.I. 2017/692, regulation 50 and 52.

[85] Ibid., regulation 50(3).

[86] G Ryle et al, 'Banking Giant HSBC Sheltered Murky Cash Linked to Dictators and Arms Dealers', (International Consortium for Investigative Journalists, 8 February 2015) <https://www.icij.org/investigations/swiss-leaks/banking-giant-hsbc-sheltered-murky-cash-linked-dictators-and-arms-dealers/ > accessed 10th May 2022.

[87] Ibid.

[88] BBC News, 'HSBC Bank 'Helped Clients Dodge Millions in Tax' (10th February 2015) <http://www.bbc.co.uk/news/business-31248913> accessed 10th May 2022.

[89] Ibid

[90] O Bowcott, 'HSBC Should Face UK Criminal Charges, Says Former Public Prosecutor' (The Guardian, 22 February 2015) <https://www.theguardian.com/politics/2015/feb/22/hsbc-uk-criminal-charges-former-public-prosecutor-hmrc> accessed 26th April 2022.

[91] R v Shanly The Times, 5 July 2012 (Wood Green Crown Court); Public Accounts Committee, Improving Tax Collection (HC 2014-15, 974) p.12.

[92] United States Department of Justice, 'Justice Department Announces Deferred Prosecution Agreement with HSBC Private Bank (Suisse) SA' (10 December 2019) <https://www.justice.gov/opa/pr/justice-department-announces-deferred-prosecution-agreement-hsbc-private-bank-suisse-sa> accessed 9th November 2020; MM Hamilton, 'HSBC to Pay $352m to Settle Tax Evasion Charges in France (International Consortium of Investigative Journalists, 15 November 2017) <https://www.icij.org/investigations/swiss-leaks/hsbc-swiss-france-352m-settlement/> accessed 10th May 2022.

[93] 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).

[94] 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 with Respect to Taxes on Income and on Capital Gains with Protocol (Signed 19th June 2008, entered into force 18th December 2009) 2011 UKTS 005, Art.27(2).

[95] OECD, Model Tax Convention on Income and on Capital (OECD Publishing, 2017) Commentary to Art 26(2), para 12.3.

[96] Ibid.

[97] J Garside et al, 'France Says It Did Not Restrict UK From Using HSBC Files To Pursue Bank and Criminals' (The Guardian, 13 February 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 26th April 2022.

[98] Treasury Committee, Oral Evidence: Financial Conduct Authority (10 February 2015, HC 2014-15, 1055) Q75 and 76.

[99] HM Revenue & Customs, 'HMRC Confirms HSBC Suisse Bank Data Can Now Be Shared' (25 February 2015) <https://www.gov.uk/government/news/hmrc-confirms-hsbc-suisse-bank-data-can-now-be-shared> accessed 26th April 2022.

[100] Ibid.

[101] First reported by M Kleinman, 'FCA Ends Probe Into HSBC Swiss Tax Affair' (Sky News, 4 January 2016) <https://news.sky.com/story/fca-ends-probe-into-hsbc-swiss-tax-affair-10334024> accessed 26th April 2022.

[102] See J Fisher, 'HSBC, Tax Evasion and Criminal Prosecution' (2015) 1253 Tax Journal 6. This is not the first time that there was no enforcement action taken against a UK headquartered bank. See for example the response by the FSA towards HSBC following its deferred prosecution agreement from the Department of Justice in December 2012. See generally US House of Representatives, Too Big to Jail: Inside the Obama Justice Department's Decision not to Hold Wall Street Accountable (Republican Staff of the Committee on Financial Services, US House of Representatives, 2016).

[103] Anderson, D. 'Attacks in London and Manchester March-June 2017 Independent Assessment of MI5 and Police' (HM Government: 2017) at 1.

[104] 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) at 85.

[105] Ibid.

[106] See Anderson above, n 319 at 17.

[107] Ibid., at 85.

[108] Attorney General's Office Fraud Review – Final Report (Attorney General's Office: 2006).

[109] General's Office Fraud Review – Final Report (Attorney General's Office 2006, 7).

[110] Proceeds of Crime Act 2002, s. 330.

[111] It is important to note that the Proceeds of Crime Act 2002 applies to serious crime, which includes fraud.

[112] Home Office Home office circular 47/2004 priorities for the investigation of fraud cases (Home Office 2004).

[113] Attorney General's Office, Fraud Review: Final Report (2006). The Labour government announced that it intended to introduce a radical overhaul of the laws on fraud in its 2005 general election manifesto. See Labour Party, Labour Party Manifesto: Britain Forward not Back (2005).

[114] Attorney General's Office, Fraud Review: Final Report (2006), 10.

[115] A Palmer Countering Economic Crime: A Comparative Analysis (London: Routledge, 2018) p 46.

[116] B Rider, 'A bold step?' (2009) 30(1) Company Lawyer 1.

[117] M Morgan-Bentley 'Action Fraud scrapped after Time expose' (July 28 2021), available at https://www.thetimes.co.uk/article/fraud-line-scrapped-after-times-expose-n2tlkbmrv.

[118] C Mackey and J Savil Fraud A review of the national 'lead force' responsibilities of the City of London Police and the effectiveness of investigations in the UK (London: City of London, 2020).

[119] Above n 198, p 2.

[120] Ibid, at 43.

.

[121] R Syal 'Judge criticises National Crime Agency over collapse of fraud trial' (December 2 2014), available at https://www.theguardian.com/law/2014/dec/02/judge-criticises-national-crime-agency-fraud-trial.

[122] HM Inspectorate of Constabulary and Fire and Rescue Services National Crime Agency inspection An inspection of the National Crime Agency's relationship with regional organised crime units (London: HM Inspectorate of Constabulary and Fire and Rescue Services, 2019).

[123] Above n 182, p 58.

[124] S.I. 2017/692.

[125] For a more detailed discussion, see HM Treasury, Anti-Money Laundering and Counter Terrorist Financing: Supervision Report 2017–18 (2019).

[126] Proceeds of Crime Act 2002, s. 363(5). See Serious Organised Crime Agency v. Perry [2012] UKSC 35

[127] Proceeds of Crime Act 2002, s. 370(6). See R v. Zinga (Munaf Ahmed) [2014] EWCA 52.

[128] Proceeds of Crime Act 2002, s. 357. See R (on the application of KRB Inc) v. Director of the Serious Fraud Office [2021] UKSC 2.

[129] Terrorism Act 2000, s.19.

[130] Proceeds of Crime Act 2002, c. 4, §§ 330–32 (Eng).

[131] Financial Services Commission, Guidance Notes – Systems of Control to Prevent the Financial System from Being Used for Money Laundering or Terrorist Financing Activities (2011), 8.1.

[132] R v DA Silva [2006] EWCA Crim 1654. This case related to the interpretation of the phrase under the Criminal Justice Act 1988. For a more detailed discussion of the decision in this case, see G. Brown and T. Evans, 'The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicious activities' (2008), Journal of International Banking Law and Regulation, 23(5), 274–277.

[133] K v National Westminster Bank, HMRC, SOCA [2006] EWCA Civ 1039.

[134] Financial Services Commission, Guidance Notes – Systems of Control to Prevent the Financial System from Being Used for Money Laundering or Terrorist Financing Activities (2011), 8.1.

[135] Terrorism Act 2000 c. 11, sch. 6.

[136] Ibid.

[137] Ibid.

[138] Ibid.

[139] Ibid.

[140] Ibid.

[141] Terrorism Act 2000 c.11, sch. 6(5) (Eng.).

[142] Ibid.

[143] Financial Action Task Force, Private Sector Information Sharing (2017), 2.

[144] See Home Office, 'Home Secretary on the work of the Financial Sector Forum: Theresa May announces launch of Joint Money Laundering Intelligence Taskforce' (24 February 2015), www.gov.uk/government/speeches/home-secretary-on-the-work-of-the-financial-sector-forum, accessed 18 July 2018.

[145] National Crime Agency, 'National Economic Crime Centre', www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre, accessed 27 September 2021. High-end money laundering has been identified by the NCA as one of its national priorities. See National Crime Agency, NCA Annual Plan 2017–2018 (2017), 9.

[146] Financial Conduct Authority, 'Effectiveness and proportionality: our financial crime priorities – speech by Rob Gruppetta, Head of Financial Crime Department' (10 November 2016), www.fca.org.uk/news/speeches/effectiveness-proportionality-financial-crime-priorities, accessed 14 February 2019. The voluntary exchange of information sharing was introduced by the Criminal Finances Act 2017, which amended the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

[147] See AUSTRAC, 'Fintel Alliance', www.austrac.gov.au/about-us/fintel-alliance, accessed 17 February 2019.

[148] See Monetary Authority of Singapore, 'CAD and MAS partner industry stakeholders to fight financial crimes' (24 April 2017), www.mas.gov.sg/News-and-Publications/Media-Releases/2017/CAD-and-MAS-Partner-Industry-Stakeholders-to-Fight-Financial-Crimes.aspx, accessed 17 February 2019.

[149] Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce launched' (26 May 2017), www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml, accessed 2 February 2019.

[150] Financial Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures United Kingdom Mutual Evaluation Report (2018), 6.

[151] 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.

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

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

[154] Criminal Finances Act 2017, s. 11(6).

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

[156] Financial Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures United Kingdom Mutual Evaluation Report (2018), 57.

[157] See Law Commission, Anti-Money Laundering: The SARs Regime (2019), 44.

[158] 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 25 February 2019. See also Financial Conduct Authority Office for Professional Body Anti-Money Laundering Supervision (OPBAS), Sourcebook for Professional Body Anti-Money Laundering Supervisors (2018), 19, 20. For a brief discussion, see Royal United Service Institute for Defence and Security Studies, Known Unknowns Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers (2018).

[159] Financial Action Task Force, Anti-Money Laundering and Counter-Terrorist Financing Measures United Kingdom Mutual Evaluation Report (2018), 165.

[160] HM Treasury and Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2017 (2017), ch. 6.

[161] HM Treasury and Home Office, National Risk Assessment of Money Laundering and Terrorist Financing 2017 (2017), ch. 7. See also Financial Action Task Force, Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals (2013).

[162] See HM Government, 'Estate agents targeted in money laundering crackdown' (4 March 2019), www.gov.uk/government/news/estate-agents-targeted-in-money-laundering-crackdown, accessed 14 March 2019.

[163] Law Commission, Anti-Money Laundering: The SARs Regime Consultation Paper (2018), 174.

[164] Law Commission, Anti-Money Laundering: The SARs Regime Consultation Paper (2018), 44.

[165] Law Commission, Anti-Money Laundering: The SARs Regime Consultation Paper (2018), 166.

[166] Serious Fraud Office 'Asil Nadir found guilty' (August 22 2012), available at https://www.sfo.gov.uk/2012/08/22/asil-nadir-found-guilty/.

[167] Department of Trade and Industry Robert Maxwell and Mirror Group Pensions (London: Department of Trade and Industry, 2001).

[168] Department of Trade and Industry Guinness PLC (London: Department of Trade and Industry, 1997).

[169] Parliamentary Commissioner for Administration The Barlow Clowes Affair (London: Parliamentary Commissioner for Administration, 1998).

[170] HM Treasury Select Committee Fixing LIBOR: some preliminary findings (London: HM Treasury Select Committee, 2012).

[171] National Audit Office Implementing employment support schemes in response to the COVID-19 pandemic (London: National Audit Office: 2020) pp 42-58.

[172] The calculation of fraud is fraught with methodological difficulties. See M Levi and J Burrows 'Measuring the impact of fraud in the UK: a conceptual and empirical journey' (2008) 48(3) British Journal of Criminology, 293.

[173] National Fraud Authority Annual Fraud Indicator 2010 (London: National Fraud Authority, 2010) p 3.

[174] National Fraud Authority Annual Fraud Indicator 2012 (London: National Fraud Authority, 2012) p 3.

[175] National Fraud Authority Annual Fraud Indicator 2013 (London: National Fraud Authority, 2013).

[176] National Crime Agency 'Fraud' (n/d), available at https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime.

[177] J Gee and M Button The Financial Cost of Fraud 2019 The latest data from around the world (Portsmouth: Crowe and Portsmouth University, 2019) p 6-7.

[178] HM Government Beating crime plan – fewer victims, peaceful neighbourhoods, safe country (London: HM Government, 2021) p 61.

[179] Home Office Home office circular 47/2004 priorities for the investigation of fraud cases (Home Office, London, 2004).

[180] FCA Handbook SUP15.3.17R

[181] Ibid, SUP 15.7.3.

[182] Ibid.

[183] See Goldstraw-White, J. and Gill, M. The mandatory reporting of fraud: Finding solutions and sharing best practice (Fraud Advisory Panel: 2021) p 8..

[184] Ibid, p 9.

[185] Serious Crime Act 2007, s. 68.

[186] Home Office Data sharing for the prevention of fraud – Code of Practice for public authorities disclosing information to a specified anti-fraud organisations under sections 68 to 72 of the Serious Crime Act 2007 (Home Office: 2016) 20.

[187] Serious Crime Act 2007, s, 68(8).

[188] Home Office Data sharing for the prevention of fraud – Code of Practice for public authorities disclosing information to a specified anti-fraud organisations under sections 68 to 72 of the Serious Crime Act 2007 (Home Office: 2016) 20.

[189] 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 10th April 2021.

[190] 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 10th April 2021.

[191] 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.

[192] Ibid.

[193] Finance Act 2007, s.82-87.

[194] Police and Criminal Evidence Act 1984, Schedule 1, s.14(2).

[195] 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.

[196] Ibid.

[197] A Craggs, 'Beware of the Knock' (2017) 180(4617) Taxation 11, 13.

[198] Serious Organised Crime and Police Act 2005, ss.60-70.

[199] Ibid, s.67.

[200] Police and Criminal Evidence Act 1984, s.8, s.114.

[201] Finance Act 2013, s.224, Schedule 48.

[202] Police and Criminal Evidence Act 1984, s.8, s.114.

[203] Police and Criminal Evidence Act 1984, s.24, s.32.

[204] Police and Criminal Evidence Act 1984 (Application to Revenue and Customs) Order 2015, SI 2015/1783, Art 4.

[205] HM Revenue & Customs, 'Guidance: HMRC's Criminal Investigation Powers and Safeguards' (13 May 2019) <https://www.gov.uk/government/publications/criminal-investigation/criminal-investigation> accessed 9th April 2021.

[206] Contained in the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000 and the Police Act 1997, ibid. A Craggs, 'Caught in the Act' (2021) 187(4786) 24, 25.

[207] Proceeds of Crime Act 2002, s.340.

[208] Ibid, s330-332.

[209] 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' (HMIC, 2014) <https://www.justiceinspectorates.gov.uk/hmicfrs/wp content/uploads/hmrc-proceeds-of-crime-revisit.pdf> accessed 14th March 2020 p.30. It is 'a major user of SAR information' HMRC Officer Jonathan Chapman cited in National Crime Agency, 'SARs in Action' (Issue 1, March 2019) <https://nationalcrimeagency.gov.uk/who-we-are/publications/268-ukfiu-sars-in-action-march-2019> accessed 14th March 2020, at p.7.

[210] 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' (HMIC, 2011) <https://www.justiceinspectorates.gov.uk/hmicfrs/media/hmrc-proceeds-of-crime-inspection-20110712.pdf> accessed 14th March 2020, p.32; 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' (HMIC, 2014) <https://www.justiceinspectorates.gov.uk/hmicfrs/wp content/uploads/hmrc-proceeds-of-crime-revisit.pdf> accessed 14th March 2020, p.30.

[211] T Monger, 'Pointless POCA?' (2014) 174 Taxation 8.

[212] National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2014' <https://www.octf.gov.uk/OCTF/media/OCTF/images/publications/SARS-Annual-Report-2014.pdf?ext=.pdf> accessed 14th March 2020, at p.24.

[213] In addition, 'A further £9,408,865 was generated from enhancing HMRC cases already under civil investigation by providing intelligence in SARs.' National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2019' <https://nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019 > accessed 16th May 2022, at p.11.

[214] "A further £7,072,085 was generated from enhancing HMRC cases already under civil investigation by providing intelligence in SARs." National Crime Agency, 'Suspicious Activity Reports (SARs) Annual Report 2020' <https://nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019 > accessed 16th May 2022, at p.18.

[215] SE Williams, '£80m of British Taxpayers' Money 'Funnelled to Al-Qaeda' in Decades-Long Scam' (The Telegraph, 31 March 2019) <https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled-al-qaeda-decades-long/> accessed 14th May 2022.

[216] See generally, O Mba, 'Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality' [2012] 2 BTR 187.

[217] R v Inland Revenue Comrs, Ex p National Federation of Self-Employed and Small Businesses Ltd [1982] AC 617, 633.

[218] E McNicholas, 'Revenue and Customs Act 2005 — Powers and Disclosure' (2005) 26(20) PTN 153.

[219] Commissioners for Revenue and Customs Act 2005, s.19(4).

[220] Ibid, s.18(2)(a)

[221] 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, dated 19th October 2011).

[222] R (on the application of Ingenious Media Holdings Plc) v Revenue and Customs Commissioners [2016] UKSC 54.

[223] Commissioners for Revenue and Customs Act 2005, s.18(2).

[224] Ibid, s.18(2)(b), s.21.

[225] Ibid, s.18(2)(b), s.20.

[226] Ibid, s.20(4)-(6).

[227] HM Revenue & Customs, 'HMRC Internal Manual: IDG40340 - Sharing Information Outside of HMRC: Lawful Disclosure: Public Interest Disclosure (Updated 25 February 2022) <https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg40340> accessed 14th May 2022.

[228] Commissioners for Revenue and Customs Act 2005, s.18(3).

[229] 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' (Updated 25th February 2022) <https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg50140> accessed 14th May 2022.

[230] Financial Services and Markets Act 2000, s.350.

[231] 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, dated 19th October 2011).

[232] 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).

[233] Committee of Public Accounts, HM Revenue & Customs 2010–11 Accounts: Tax Disputes (HC 2010–12, 1531-I) p.9.

[234] M Hodge, Called to Account: How Governments and Vested Interests Combine to Waste Our Money (Little, Brown 2016) Chapter 2.

[235] 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.

[236] Commissioners for Revenue & Customs Bill Deb 11 January 2005, Col 64.

[237] Hodge (n 296).

[238] 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 14th May 2022.

[239] FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report' (December 2018) <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 10th May 2022, p.57.

[240] HM Government, 'United Kingdom Anti-Corruption Strategy 2017-2022: Year 3 Update – 2020' (16 December 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 12th May 2022, p.13.

[241] Ibid.

[242] Ibid.

[243] Ibid.

Bibliography

HM Government, 'United Kingdom Anti-Corruption Strategy 2017-2022: Year 3 Update – 2020' (16 December 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 12th May 2022

'GDPR for litigators' *Allen & Overy Blog*, accessible at: https://www.allenovery.com/en-gb/global/news-and-insights/publications/gdpr-for-litigators-2019.

A Craggs, 'Beware of the Knock' (2017) 180(4617) Taxation 11, 13.

A Craggs, 'Caught in the Act' (2021) 187(4786) 24, 25.

A Palmer Countering Economic Crime: A Comparative Analysis (London: Routledge, 2018) p 46.

A Wells, 'No, No, No!' (2010) 166(4272) Taxation 6,7.

A. Leong, 'Chasing dirty money: domestic and international measures against money laundering' (2007), *Journal of Money Laundering Control*, 10(2), 140–156, at 142.

Anderson, D. 'Attacks in London and Manchester March-June 2017 Independent Assessment of MI5 and Police' (HM Government: 2017) at 1.

Attorney General's Office *Fraud Review – Final Report* (Attorney General's Office: 2006).

AUSTRAC, 'Fintel Alliance', www.austrac.gov.au/about-us/fintel-alliance, accessed 17 February 2019.

B Rider, 'A bold step?' (2009) 30(1) Company Lawyer 1.

BBC News, 'HSBC Bank 'Helped Clients Dodge Millions in Tax' (10th February 2015) <http://www.bbc.co.uk/news/business-31248913> accessed 10th May 2022.

C Mackey and J Savil Fraud A review of the national 'lead force' responsibilities of the City of London Police and the effectiveness of investigations in the UK (London: City of London, 2020).

College of Policing, 'Information Sharing' accessible at: https://www.college.police.uk/app/information-management/information-sharing

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, dated 19th October 2011).

Department of Digital Culture, Media and Sport and Rt. Hon Nadine Dorries (17 June 2022) at: https://www.gov.uk/government/news/new-data-laws-to-boost-british-business-protect-consumers-and-seize-the-benefits-of-brexit.

Department of Trade and Industry *Guinness PLC* (London: Department of Trade and Industry, 1997).

Department of Trade and Industry *Robert Maxwell and Mirror Group Pensions* (London: Department of Trade and Industry, 2001).

Diane Zimmerman, 'Requiem for a Heavyweight: A farewell to Warren and Brandeis's privacy tort' (1983) 68(2) *Cornell Law Review* 291, 326

E McNicholas, 'Revenue and Customs Act 2005 — Powers and Disclosure' (2005) 26(20) PTN 153.

FATF, 'Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report' (December 2018) <https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf> accessed 10th May 2022.

Financial Action Task Force Anti-money laundering and counter-terrorist financing measures United Kingdom Mutual Evaluation Report (Financial Action Task Force: Paris, 2018)

Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures United Kingdom Mutual Evaluation Report* (2018).

Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures United Kingdom Mutual Evaluation Report* (2018), 6.

Financial Action Task Force, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (2013).

Financial Action Task Force, *Private Sector Information Sharing* (2017), 2.

Financial Conduct Authority 'FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings', January 1 2017, available from https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure, accessed June 16 2022.

Financial Conduct Authority 'FCA fines HSBC Bank plc £63.9 million for deficient transaction monitoring controls', December 17 2021, available from https://www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls, accessed June 6 2022.

Financial Conduct Authority 'NatWest fined £264.8 million for anti-money laundering failures', December 13 2021, available from https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures#:~:text=NatWest%20failed%20to%20comply%20with,money%20laundering%20and%20terrorist%20financing

Financial Conduct Authority Office for Professional Body Anti-Money Laundering Supervision (OPBAS), *Sourcebook for Professional Body Anti-Money Laundering Supervisors* (2018).

Financial Conduct Authority, 'Effectiveness and proportionality: our financial crime priorities – speech by Rob Gruppetta, Head of Financial Crime Department' (10 November 2016), www.fca.org.uk/news/speeches/effectiveness-proportionality-financial-crime-priorities, accessed 14 February 2019.

Financial Services Commission, *Guidance Notes – Systems of Control to Prevent the Financial System from Being Used for Money Laundering or Terrorist Financing Activities* (2011), 8.1.

Fiona Brimblecombe, 'The Public Interest in Deleted Personal Data? The Right to be Forgotten's Freedom of Expression Exceptions Examined through the Lens of Article 10 ECHR' (2020) 23(1) *Journal of Internet Law* 1-29.

G Ryle et al, 'Banking Giant HSBC Sheltered Murky Cash Linked to Dictators and Arms Dealers', (International Consortium for Investigative Journalists, 8 February 2015) <https://www.icij.org/investigations/swiss-leaks/banking-giant-hsbc-sheltered-murky-cash-linked-dictators-and-arms-dealers/ > accessed 10th May 2022.

G. Brown and T. Evans, 'The impact: the breadth and depth of the anti-money laundering provisions requiring reporting of suspicious activities' (2008), *Journal of International Banking Law and Regulation*, 23(5), 274–277.

General's Office *Fraud Review – Final Report* (Attorney General's Office 2006, 7).

Goldstraw-White, J. and Gill, M. *The mandatory reporting of fraud: Finding solutions and sharing best practice* (Fraud Advisory Panel: 2021.

Goodchild, S. 'The mystery of the London bomber and his secret wealth', June 8 2006, available from https://www.independent.co.uk/news/uk/crime/the-mystery-of-the-london-bomber-and-his-secret-wealth-522102.html, accessed June 19 2020.

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' (HMIC, 2014) <https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/hmrc-proceeds-of-crime-revisit.pdf> accessed 14th March 2020.

HM Government *Beating crime plan – fewer victims, peaceful neighbourhoods, safe country* (London: HM Government, 2021).

HM Government, 'Estate agents targeted in money laundering crackdown' (4 March 2019), www.gov.uk/government/news/estate-agents-targeted-in-money-laundering-crackdown, accessed 14 March 2019.

HM Inspectorate of Constabulary and Fire and Rescue Services National Crime Agency inspection An inspection of the National Crime Agency's relationship with regional organised crime units (London: HM Inspectorate of Constabulary and Fire and Rescue Services, 2019).

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 10th April 2021.

HM Revenue & Customs, 'Guidance: HMRC's Criminal Investigation Powers and Safeguards' (13 May 2019) <https://www.gov.uk/government/publications/criminal-investigation/criminal-investigation> accessed 9th April 2021.

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 10th April 2021.

HM Revenue & Customs, 'HMRC Confirms HSBC Suisse Bank Data Can Now Be Shared' (25 February 2015) <https://www.gov.uk/government/news/hmrc-confirms-hsbc-suisse-bank-data-can-now-be-shared> accessed 26th April 2022.

HM Revenue and Customers 'HMRC Internal Manual Information Disclosure Guide', March 19 2016, available from https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg50140, accessed June 19 2020.

HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (2017).

HM Treasury and Home Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (2017).

HM Treasury Select Committee *Fixing LIBOR: some preliminary findings* (London: HM Treasury Select Committee, 2012).

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 25 February 2019.

HM Treasury, *Anti-Money Laundering and Counter Terrorist Financing: Supervision Report 2017–18* (2019).

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 14th May 2022.

Home Office *Data sharing for the prevention of fraud – Code of Practice for public authorities disclosing information to a specified anti-fraud organisations under sections 68 to 72 of the Serious Crime Act 2007* (Home Office: 2016) 20.

Home Office *Data sharing for the prevention of fraud – Code of Practice for public authorities disclosing information to a specified anti-fraud organisations under sections 68 to 72 of the Serious Crime Act 2007* (Home Office: 2016).

Home Office *Home office circular 47/2004 priorities for the investigation of fraud cases* (Home Office, London, 2004).

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

Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce launched' (26 May 2017), www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml, accessed 2 February 2019.

Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

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) at 85.

J Fisher, 'HSBC, Tax Evasion and Criminal Prosecution' (2015) 1253 Tax Journal 6.

J Garside et al, 'France Says It Did Not Restrict UK From Using HSBC Files To Pursue Bank and Criminals' (The Guardian, 13 February 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 26th April 2022.

J Gee and M Button *The Financial Cost of Fraud 2019 The latest data from around the world* (Portsmouth: Crowe and Portsmouth University, 2019).

KPMG, *Money Laundering: Review of the Reporting System* (2003), 14.

KPMG, *Money Laundering: Review of the Reporting System* (2003), 14.

Law Commission, *Anti-Money Laundering: The SARs Regime* (2019), 44.

Law Commission, *Anti-Money Laundering: The SARs Regime Consultation Paper* (2018), 174.

M Hodge, *Called to Account: How Governments and Vested Interests Combine to Waste Our Money* (Little, Brown 2016) Chapter 2.

M Kleinman, 'FCA Ends Probe Into HSBC Swiss Tax Affair' (Sky News, 4 January 2016) <https://news.sky.com/story/fca-ends-probe-into-hsbc-swiss-tax-affair-10334024> accessed 26th April 2022.

M Morgan-Bentley 'Action Fraud scrapped after Time expose' (July 28 2021), available at https://www.thetimes.co.uk/article/fraud-line-scrapped-after-times-expose-n2tlkbmrv.

Mark J Taylor, 'Data Protection: Too Personal to Protect?' (2006) 3(1) *SCRIPT-ed* 72, 75

Mba, O. 'Transparency and accountability of tax administration in the UK: the nature and scope of taxpayer confidentiality' (2012) British Tax Review, 2, 187-225.

Ministry of Justice, 'part 31 - disclosure and inspection of documents' accessible at: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part31.

MM Hamilton, 'HSBC to Pay $352m to Settle Tax Evasion Charges in France (International Consortium of Investigative Journalists, 15 November 2017) <https://www.icij.org/investigations/swiss-leaks/hsbc-swiss-france-352m-settlement/> accessed 10th May 2022.

Monetary Authority of Singapore, 'CAD and MAS partner industry stakeholders to fight financial crimes' (24 April 2017), www.mas.gov.sg/News-and-Publications/Media-Releases/2017/CAD-and-MAS-Partner-Industry-Stakeholders-to-Fight-Financial-Crimes.aspx, accessed 17 February 2019.

Mushtaq, W. 'Imran Hussain's father says not responsible for Scottish-Pakistani son's £300m fraud', November 24 2019, available from https://www.geo.tv/latest/258285-imran-hussains-father-says-not-responsible-for-scottish-pakistani-sons-300m-fraud, accessed June 22 2020.

National Audit Office *Implementing employment support schemes in response to the COVID-19 pandemic* (London: National Audit Office: 2020).

National Crime Agency 'Fraud' (n/d), available at https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime.

National Crime Agency, 'National Economic Crime Centre', www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre, accessed 27 September 2021. High-end money laundering has been identified by the NCA as one of its national priorities.

National Crime Agency, *NCA Annual Plan 2017–2018* (2017), 9.

National Crime Agency, *SARs Annual Report 2017* (2017), 6. (There was no 2015–2016 report.)

National Crime Agency, *SARs Annual Report 2018* (2018), 3.

National Crime Agency, *SARs Annual Report 2019* (2019), 4.

National Crime Agency, *SARs Annual Report 2020* (2020), 4.

National Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2013* (2013), 6.

National Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2014* (2014), 7.

National Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2015* (2015), 7.

National Fraud Authority *Annual Fraud Indicator 2010* (London: National Fraud Authority, 2010).

National Fraud Authority *Annual Fraud Indicator 2012* (London: National Fraud Authority, 2012).

National Fraud Authority *Annual Fraud Indicator 2013* (London: National Fraud Authority, 2013).

O Bowcott, 'HSBC Should Face UK Criminal Charges, Says Former Public Prosecutor' (The Guardian, 22 February 2015) <https://www.theguardian.com/politics/2015/feb/22/hsbc-uk-criminal-charges-former-public-prosecutor-hmrc> accessed 26th April 2022.

O Butler, 'Official Secrecy and the Criminalisation of Unauthorised Disclosures' (2022) 138 LQR 273, 276.

O Mba, 'Transparency and Accountability of Tax Administration in the UK: The Nature and Scope of Taxpayer Confidentiality' [2012] 2 BTR 187.

OECD *Whole of Government Approaches to Fragile States* (OECD: 2006) at 29.

OECD, *Model Tax Convention on Income and on Capital* (OECD Publishing, 2017).

Parliamentary Commissioner for Administration *The Barlow Clowes Affair* (London: Parliamentary Commissioner for Administration, 1998).

Paul De Hert and Vagelis Papakonstantinou, 'The proposed Data Protection Regulation replacing Directive 95/46/EC: a sound system for the protection of individuals' (2012) 28(2) Computer Law & Security Review 130,183.

Paul Wragg, 'Protecting private information of public interest: Campbell's great promise, unfulfilled' (2015) 7(2) *Journal of Media Law* 225.

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).

Public Accounts Committee, *Oral Evidence: Tax Avoidance and Evasion: HSBC* (23 March 2015, HC 2014-15 1095-I)

R Brockwell, L McKeown, 'No More Mr Nice Guy?' (2003) 151(3913) Taxation 350.

R Syal 'Judge criticises National Crime Agency over collapse of fraud trial' (December 2 2014), available at https://www.theguardian.com/law/2014/dec/02/judge-criticises-national-crime-agency-fraud-trial.

R. Sarker, 'Anti-money laundering requirements: too much pain for too little gain' (2006), *Company Lawyer*, 27(8), 250–251, at 251.

Rebecca Moosavian, 'A just balance or just imbalance? The role of metaphor in misuse of private information' (2015) 7(2) *Journal of Media Law* 196, 217

Royal United Service Institute for Defence and Security Studies, *Known Unknowns Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers* (2018).

SE Williams, '£80m of British Taxpayers' Money 'Funnelled to Al-Qaeda' in Decades-Long Scam' (The Telegraph, 31 March 2019) <https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled-al-qaeda-decades-long/> accessed 14th May 2022.

SE Williams, '£80m of British Taxpayers' Money 'Funnelled to Al-Qaeda' in Decades-Long Scam' (The Telegraph, 31 March 2019) <https://www.telegraph.co.uk/news/2019/03/31/80m-british-taxpayers-money-funnelled-al-qaeda-decades-long/> accessed 14th May 2022.

See Home Office, 'Home Secretary on the work of the Financial Sector Forum: Theresa May announces launch of Joint Money Laundering Intelligence Taskforce' (24 February 2015), www.gov.uk/government/speeches/home-secretary-on-the-work-of-the-financial-sector-forum, accessed 18 July 2018.

M Levi and J Burrows 'Measuring the impact of fraud in the UK: a conceptual and empirical journey' (2008) 48(3) British Journal of Criminology, 293.

Serious Fraud Office 'Asil Nadir found guilty' (August 22 2012), available at https://www.sfo.gov.uk/2012/08/22/asil-nadir-found-guilty/.

Serious Organised Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2010* (2010).

Serious Organised Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2011* (2011).

Serious Organised Crime Agency, *The Suspicious Activity Reports Regime Annual Report 2012* (2012).

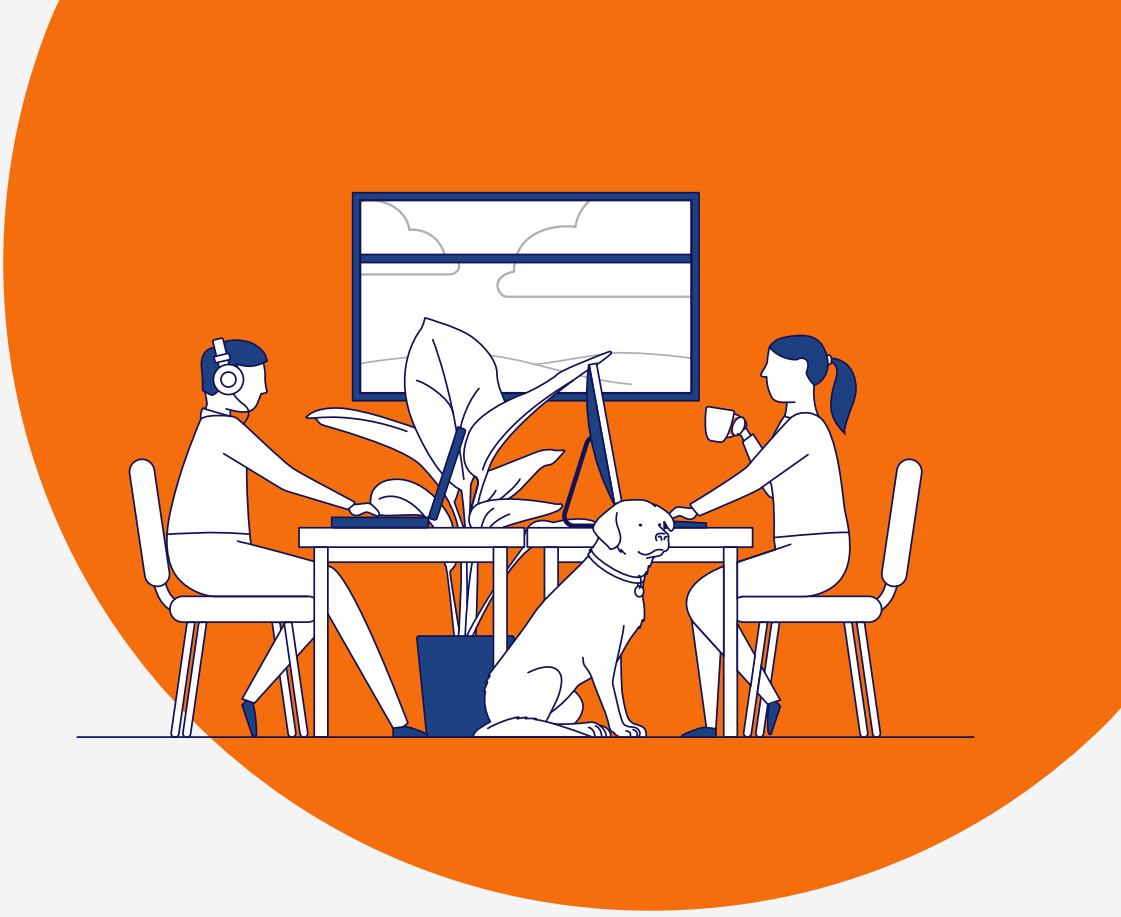
T Monger, 'Pointless POCA?' (2014) 174 Taxation 8.

Information Commissioner's Office Guidance, 'Sharing Personal Data with Law Enforcement Authorities' accessible at: https://ico.org.uk/for-organisations/data-sharing-information-hub/sharing-personal-data-with-law-enforcement-authorities/.

Treasury Committee, *Oral Evidence: Financial Conduct Authority* (10 February 2015, HC 2014-15, 1055).

United States Department of Justice, 'Justice Department Announces Deferred Prosecution Agreement with HSBC Private Bank (Suisse) SA' (10 December 2019) <https://www.justice.gov/opa/pr/justice-department-announces-deferred-prosecution-agreement-hsbc-private-bank-suisse-sa> accessed 9th November 2020#

US House of Representatives, Too Big to Jail: Inside the Obama Justice Department's Decision not to Hold Wall Street Accountable (Republican Staff of the Committee on Financial Services, US House of Representatives, 2016).



Drop us a line if you would like to know more about any of the topics raised in the whitepaper or how Synalogik is helping information sharing and automation in the public sector.

Public Sector Team

public.sector@synalogik.com