THE LEGAL AND INSTITUTIONAL INFRASTRUCTURE OF ANTI-MONEY LAUNDERING IN THE UK: A REPORT FOR THE CULLEN COMMISSION

Professor Michael LEVI, CARDIFF UNIVERSITY

I. INTRODUCTION

HISTORY OF ANTI-MONEY LAUNDERING IN THE UK

The history of anti-money laundering (AML) efforts will be divided into two sections: criminalisation of money laundering, and preventative control efforts.

– *Criminalisation of Money Laundering*

The rise in political and perhaps social consciousness of money laundering is an impressive phenomenon, but its manifestations reflect what mobilisation can be brought to bear politically, which varies between countries and over time. The UK's legislative AML efforts began formally with the Drug Trafficking Offences Act 1986, which introduced drugs-only money laundering offences, in keeping with the view that drug trafficking was the most serious and fastest-growing problem connected with "organised crime": indeed it is arguable that this was what organised crime meant and even still means in most parts of the world..[1] Since the late 1980s, the UK (and the world) has witnessed an extraordinary growth in efforts to control crime for economic and political gain (and, especially since '9/11', terrorism) via measures to identify, freeze and confiscate the proceeds of crime nationally and transnationally. What follows is a review of how the UK approached these control issues and what we know about the effects of these controls, which are mainly input and output efficiency rather than effectiveness measures.[2]

– *Development of the AML Preventive-Regulatory Regime*

There was an informal suspicious transaction reporting process before 1986 based around personal relationships and trust, notwithstanding the confidentiality rules in *Tournier*.[3] After the Drug Trafficking Offences Act 1986, informal reporting by some bankers increased as the legislation created a defence for an individual involved in an arrangement that facilitates another

---

[1] There was not seen to be any need in the UK to criminalise organised crime membership *per se* because the conspiracy legislation was considered adequate to the task and because there was substantial opposition to the use of wiretaps in evidence, which is often required to prove membership. See Michael Levi and Alaster Smith, *A comparative analysis of organised crime conspiracy legislation and practice and their relevance to England and Wales*, London: Home Office, 2002. Nevertheless, under EU pressure, participation in the criminal activities of an organised crime group ('OCG') was criminalised under section 45 of the Serious Crime Act 2015 ('SCA'), though very rarely prosecuted, as has also been the case in other EU countries (RAND Europe unpublished research, European Commission). See further, for the approach in the UK, https://www.cps.gov.uk/legal-guidance/organised-crime-group-participating-activities. Canada has its own political and legal history with organised crime conspiracies, which lies outside my brief to discuss.

[2] See more generally, Michael Levi and Liliya Gelemerova, 'Money laundering controls in the UK'. In Ben Vogel and Jean-Baptiste Maillart (eds.) *National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulatory Law and Data Protection*, The Hague: Intersentia, 2020.

[3] Michael Levi, *Pecunia non olet*: cleansing the money launderers from the Temple, *Crime, Law, and Social Change*, 16, (1991) 217-302.

person in retaining or controlling the proceeds of drug trafficking if that individual were to disclose their suspicion or belief to a constable. To try to coordinate financial sector behaviour and reduce the occasional tensions between police and banks, a public-private body – the Joint Money Laundering Steering Group – was set up in 1990, in collaboration with their (then) regulator, the Bank of England, to produce formal Money Laundering Guidance for the financial sector. This (nowadays superintended by HM Treasury) produced regularly updated guidance on the various Money Laundering Regulations which were promulgated and enhanced, often in response to EU Directives. In the event of civil and criminal cases, this guidance would be taken into account by the courts as a guide to best practice.

The preventive obligations imposed by the law applied to all persons in their business capacity, including solicitors; the Money Laundering Regulations 1993 applied to solicitors carrying on regulated activities under the Financial Services and Markets Act. The Criminal Justice Act and the Money Laundering Regulations introduced in 1993 made mandatory the previously voluntary reporting of non-drugs related "suspicious activity"[4]. The UK's AML and counter-terrorist financing framework consists of primary and secondary legislation and industry guidance. Industry guidance has no *direct* legal applicability, but it is admissible in court and in regulatory adjudications as evidence of 'best practice'. There has been little or no experience of how this operates in practice

The Proceeds of Crime Act 2002 (POCA) introduced a range of substantive criminal law aimed at strengthening crime proceeds recovery. This also included provisions that aimed at strengthening the AML regime. The Act (Part 7) – as amended by subsequent legislation – contains the principal (also known as "primary") AML legislation. It has been amended several times since its introduction, most particularly by the Serious Organised Crime and Police Act 2005, the Serious Crime Act 2007, the Serious Crime Act 2015 and the Criminal Finances Act 2017. The key change in regards to the AML regime was introduced by the Serious Organised Crime and Police Act 2005 which established the Serious Organised Crime Agency (SOCA), until 7 October 2013 when it was, in turn, replaced by the National Crime Agency (NCA), which houses the UK Financial Intelligence Unit. The Money Laundering Regulations 2003 brought within the regulated sector the category of "legal or natural persons acting in the exercise of their professional activities" (designated non-financial businesses and professions, DNFBPs).

Different banks and other regulated persons including law firms then and now took different approaches to the amount of internal filtering of suspicions they undertook before reporting (or not reporting) to the Financial Intelligence Unit (FIU), though these are nowhere codified. Law

[4] A more analytically accurate term would be "suspected activity", since "suspicious" implies that there is something inherent in the activity that provokes the report.

firms will be dealt with separately but as elsewhere in the world, Legal Professional Privilege is a constraint on reporting, but there have been changes in the conditions under which it applies. This may be viewed by some as inconsistency of approach, but by others as reflecting the thinking behind the shift from rules-based to risk-based or principles-based reporting, which in theory enabled diversity of judgements.

POCA and the Terrorism Act 2000[5] are supported by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (referred to as Money Laundering Regulations 2017), which set out a number of obligations for the regulated sector that are aimed at preventing or detecting money laundering and terrorist financing risk. These include the requirement for each firm (including law firms) to conduct a money laundering and terrorist financing risk assessment, to set up internal controls, train staff and implement due diligence measures. The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 came into force 10 January 2020, creating, among other things, further risk factors to assess, including whether transactions related to oil, arms, precious metals, tobacco products, cultural artefacts, ivory and other items related to protected species, or other items of archaeological, historical, cultural and religious significance, or of rare scientific value,[6] when assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate that risk. Further enhancements include lowering thresholds for due diligence in e-money products, and requiring firms to report to Companies House discrepancies between the information the firm holds on their customers compared with the information held in the Companies House Register: the aim was to remedy the false information that may be found there, since Companies House does not currently vet their accuracy (but will do so in future).[7] Obliged entities also need to understand the ownership and control structure of their corporate customers, and record any difficulties encountered in identifying beneficial ownership. Enhanced due diligence now explicitly includes any customer or transaction where either of the parties to the transaction is established in a high-risk third country (as defined by the European Commission

[5] Since 2000 there have been a series of amendments and further acts aimed at terrorism, including the Anti-Terrorism, Crime and Security Act (ATCSA) of 2001. POCA and ATCSA have been amended by the Criminal Finances Act 2017. The National Crime Agency's guidance of May 2019 "Requesting a defence from the NCA under POCA and TACT" refers to the Terrorism Act 2000 (TACT).

[6] Some AML professionals and businesses already considered these as high risk factors, from a smuggling, corruption, terrorist financing and money laundering perspective. The new enhancement in principle helps to achieve a more consistent approach across regulated persons: but this depends on implementation.

[7] (SI 2019/1511). See also https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations. Reforms to Companies House have been agreed by HMG in September 2020 following the Corporate Transparency and Register Reform consultation: compulsory identity verification ; and greater powers to query, investigate and remove false information.

in the Fourth Anti-Money Laundering Directive). Additionally, where the customer (a) is the beneficiary of a life insurance policy, (b) is a legal person or a legal arrangement, and (c) presents a high risk of money laundering or terrorist financing for any other reason, an obliged entity that is a credit or financial institution must take reasonable measures to identify and verify the identity of the beneficial owners of that beneficiary before any payment is made under the policy.

The 2019 updates also added to the list of obliged entities (defined as 'relevant persons' in UK legislation) the following: letting agents, art market participants and cryptoasset exchange providers. The requirement for an obliged entity to establish and maintain, throughout its group, policies, controls and procedures for data protection and sharing information for the purposes of preventing money laundering and terrorist financing with other members of the group, now explicitly also includes policies on the sharing of information about customers, customer accounts and transactions. In addition to training employees on AML, obliged entities now are also explicitly required to train any *agents* they use for their business.

One entirely new section concerns requests for information about accounts with credit institutions and safe-deposit boxes, whose firms must establish and maintain systems which enable them to respond, using the central automated mechanism, to requests for information from law enforcement authorities or from the Gambling Commission, which has oversight of offline and online gambling and which has adopted a vigorous approach to money laundering (though less so to 'vulnerability') supervision.[8]

In response to both public and FATF demands for greater feedback (demands observed by this author since at least 1992), the NCA can now require police or other public bodies to provide a report to it about the authority's use of that information, including the outcome of any investigations or inspections conducted on the basis of that information.[179] This may enhance the ability of the UK to report on the investigative impact of SARs and of any further intelligence development made by the FIU, though it seems unlikely that SAR makers will be given individual feedback.[180][9] This development in NCA powers is important for domestic as well as for international accountability and legitimacy, but this does not require *routine* reporting back, and agencies do not often volunteer evidence (in this case, about lack of follow up on SARs) that will likely generate serious criticism.

Current Concerns and Reform Agenda

[8] For a critical Public Accounts Committee Report, see https://publications.parliament.uk/pa/cm5801/cmselect/cmpubacc/134/134.pdf

[9] It remains to be seen how the various industry associations, including the JMLSG, will interpret the 2019 amendments and guide the regulated sector.

– *Beneficial Ownership Register*

The UK has registers of beneficial ownership for three different types of assets: companies, properties and land, and trusts. Information on the beneficial ownership of companies is publicly available. For properties owned by overseas companies and legal entities, the government plans to launch a public beneficial ownership register in 2021. The register for trusts is not public, nor is it planned to make it so.[10]

The register of beneficial owners of companies as well as properties and unexplained wealth orders[11] are among the key measures the UK has introduced in response to criticism that the UK is a key crime proceeds destination. Scholars, NGOs (e.g. Transparency International UK, Global Witness, Spotlight on Corruption and Shadow World Investigations) and practitioners have raised questions about the effectiveness of UK's AML regime and the credibility of FATF's very positive overall evaluation in relation to these reforms.[12] Subject to reforms agreed September 18 2020, Companies House has never had either the resources or the role of checking the veracity of data sent to it – for the beneficial ownership or other registers – but external bodies may be unaware of this fact.[13] Furthermore the issue has raised tensions between the UK and its overseas territories over the attempts to impose public registers on them with more stringent requirements than those done in the UK.

According to a Europol report published on 5 September 2017, the UK is one of the top countries from which both individuals and companies feature most in STRs/SARs across the EU:

> "This may be related to a perceived increasing use of UK LLPs in money laundering schemes, given that there is some scope to conceal beneficial ownership through designating ownership to entities located in jurisdictions with significant banking secrecy (i.e. on the face of it the company may appear to be a UK company, however ultimate ownership details will in fact rest elsewhere). This

[10] Federiko Mor, "Registers of beneficial ownership", House of Commons Library, Briefing Paper No 8259, 24 August 2018, https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CBP-8259.

[11] Incorporated into UK law as part of the Criminal Finances Act 2017, an unexplained wealth order is a court order issued to compel someone to reveal the sources of their unexplained wealth. Some difficulties have been experienced by the National Crime Agency in pursuing cases: see https://globalinvestigationsreview.com/digital_assets/5177505d-8751-4434-a19e-6d931ac70bf0/Court-of-Appeal-%5b1%5d.pdf, as predicted also by Levi (2018).

[12] Ron Pol, "Ron Pol reflects on effectiveness issues revealed by the UK's leaked AML/CFT evaluation & shares new visualisations of the ratings methodology that will be used to assess NZ's regime", interest.co.nz, 20 October 2018, https://www.interest.co.nz/opinion/96510/ron-pol-reflects-effectiveness-issues-revealed-uk%E2%80%99s-leaked-amlcft-evaluation-shares.

[13] In September 2019, Company Watch, which provides credit reports on thousands of private companies every year, added a disclaimer to its assessments amid fears that the Companies Register is being used by fraudsters. Among faults are that directors who misspell their names may appear multiple times. Also, companies with turnover less than £10.2m – the vast majority of those registered – can claim exemption from audits of their annual accounts. Companies House cannot currently remove bankrupt directors from their register: they have to ask them to resign.

> issue has already been addressed through the recent UK Small Business Enterprise and Employment Act 2015, which requires most UK companies, including LLPs, to maintain registers of persons with significant control over a company (essentially a register of beneficial owners)."[14]

Although this is administrative data, it has some relevance because it reflects active financial investigation in other EU countries.

Additionally, a 2019 enhancement to the Money Laundering Regulations is worth noting. Specifically, before establishing a business relationship with a company or partnership, obliged entities must:

a) collect proof of registration or an excerpt of the register from the prospective customer and
b) report to the registrar any discrepancy between information relating to the beneficial ownership of the customer which the relevant person collects (under a) above) and which otherwise becomes available to the obliged entity in the course of carrying out its duties under the Money Laundering Regulations.

It is unclear, however, how the registrar will make use of this information while guaranteeing the obliged entity's disclosure confidentiality and without the prospective customer realising that a disclosure had been made. The implications of this reporting must also be considered in the context of obliged entities having to report suspicion-triggering discrepancies to the FIU in the form of SARs. It is also unclear why the provision focuses on proof collected before the start of a business relationship, ignoring proof collected at later stages (for instance, when, during a periodic customer file review, the customer provides documents on changes).

In the context of new technologies and digital onboarding – an important component of FinTech and banking competition - obliged entities may often seek to obtain certain documentation about their prospective or existing customers from official repositories, such as company registries or exchanges, through automated software tools. This automation means that direct customer out-reach is not always necessary and is aimed at speeding up the process of on-boarding a customer or updating a customer's file. However, the 2019 enhancement to the regulations appears to require reaching out to the client for proof of registration in any event. This may defeat the purpose of automation, particularly for the entities that are on the lower end of the risk spectrum and have simpler ownership structures. It is yet to be seen how the JMLSG and other industry bodies will interpret this and other new enhancements.

[14] Europol, "From suspicion to action. Converting financial intelligence into greater operational impact", 2017, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact.

– *Statistics*

The FATF, MS and other bodies have struggled to express what they consider to be statistics that are particularly relevant to the AML outcomes that are specified (which themselves are unclear). There is no reason to suspect that UK statistics are worse than those of most other FATF countries, but the lack of comprehensive and consistent statistics has been noted by scholars and authoritative bodies.[15] The Europol report, discussed above (and the subsequent FATF Mutual Evaluation Report), highlights that the UK has not provided statistics on the financial amounts in SARs and on the conversion rate (whether a SAR has resulted in any follow-up activity, not necessarily a conviction). Such data are not collected by the UKFIU, and feedback from police and non-police bodies with SAR access has been a problem ever since the beginning of what we might term the "loose-coupled system" in the 1980s.[16] This has a policing cultural explanation not unique to the UK (and plausibly may include Canada). Busy investigators may not see it as a priority to tell the FIU when a SAR has been useful for either investigation or asset recovery purposes, and the FIU may not prioritise telling the SAR reporters even if it is notified by investigators that a SAR has been useful.[17] The FATF Evaluation criticises the UK's FIU for the absence of its own SAR follow-up investigation and for what may be described very kindly as the distributed model of sending out SARs and leaving it up to the individual recipients to investigate (or, far more often, not investigate). It should be noted that this reflects UK (or certainly England and Wales) police culture and constrained resources: this lack of internal investigation and follow-up also happens with the centralised fraud victim complaints distributed to other police forces by the National Fraud Intelligence Bureau in the City of London Police if it considers there is actionable intelligence.[18]

– *Defensive/Precautionary Reporting and Alleged Over-reporting (Over-compliance)*

[15] Michael Levi, 'Evaluating the Control of Money Laundering and Its Underlying Offences: the Search for Meaningful Data', *Asian Journal of Criminology*, 2020, 1-20; Michael Levi, Peter Reuter, and Terrence Halliday, 'Can the AML/CTF System Be Evaluated Without Better Data?' *Crime, Law and Social Change*, 69(2), 307-328. https://link.springer.com/content/pdf/10.1007%2Fs10611-017-9757-4.pdf

[16] Michael Levi, "Pecunia non olet: cleansing the money launderers from the Temple", *Crime, Law, and Social Change*, 16 (1991) 217–302; Michael Gold and Michael Levi, *Money-Laundering in the UK: an Appraisal of Suspicion-Based Reporting*, London: Police Foundation, 1994; M Levi, "Incriminating disclosures: an evaluation of money-laundering regulation in England and Wales", *European Journal of Crime, Criminal Law, and Criminal Justice*, 3(2) (1995) 202–217.

[17] Because SARs are inadmissible in criminal proceedings, reporters may not even know that a case has come to court.

[18] Alan Doig, "Fraud: from national strategies to practice on the ground – a regional case study" *Public Money & Management*, 38(2) (2018) 147–156; Home Affairs Select Committee, *Policing for the Future*, House of Commons, 2018, 515; Police Foundation, *More Than Just A Number: Improving the Police Response to Victims Of Fraud*, London: Police Foundation, 2018; HMICFRS, *Fraud: Time to choose – An inspection of the police response to fraud*, 2019; Alan Doig and Michael Levi, 'Editorial: The dynamics of the fight against fraud and bribery: reflections on core issues in this PMM theme', *Public Money and Management*, (2020) 40:5, 343-348, DOI: 10.1080/09540962.2020.1752547.

Defensive, also known in the industry as "precautionary", reporting appears to be an issue in the UK: obliged entities feel safer if they file a SAR as a precaution even where they do not know or suspect money laundering or terrorist financing but when they fear that their thought process may at a later time be subject to critical interpretation by regulators or courts. In other words, filing the SAR requires less effort than trying to prove the negative to auditors and regulators at a later stage, even though the latter proof is unlikely ever to be required.

Between 2006 and 2014, UK SARs accounted for 36% of all SARs submitted across all EU Member States. Dutch SARs accounted for 31%. SARs submitted from each of the remaining states accounted for between 1% and 5%. According to the report:

> "It is of course understandable that the UK would generate one of the highest reporting volumes in the EU: not only is it home to one of the largest financial markets in Europe, but in addition, it operates a Suspicious Activity Regime (SAR), which broadens the types of reports it can receive. Nonetheless, the figures are extremely high in comparison to other countries, which may also be a result of defensive or over reporting."

A footnote in the same Europol report further explained:

> "Although reporting guidance from the FCA, JSMLG and NCA is quite comprehensive on obligations, and the UK FIU analysis of reports suggests that the majority of the financial institutions that submit SARs conduct at least a basic level of research and analysis prior to submission, and in some cases undertake quite substantial pre-submission examination."[19]

There is some ambiguity or indeed contradiction in this perspective. The FATF pressurises countries to make more reports, and particular sectors, such as the legal and accountancy professions and estate agents, are often criticised in the media and by NGOs for making an insufficient number of reports. There is a general lack of clarity in the evaluation and enforcement community (and, for that matter, among NGOs) about what constitutes the 'right number' of reports, and there is a systemic failure to address this in terms of ratios to clear denominators. There is no consistency in the use of either numbers or percentages of reports, and little evidenced thinking about the value (indeed, the point) of firms making reports that have no serious chance of leading to action.

– *De-risking*

[19] Europol, "From suspicion to action. Converting financial intelligence into greater operational impact", 2017, https://www.europol.europa.eu/publications-documents/suspicion-to-action-converting-financial-intelligence-greater-operational-impact.

A report commissioned by the Financial Conduct Authority (FCA) and published in 2016 observes:

> "The Financial Conduct Authority … is aware that over recent years some banks have removed bank accounts/services from customers or other relationships which they associate with higher money laundering risk. This process has been termed 'de-risking' and it has been attributed to the increasing overall cost of complying with regulatory requirements. These include prudential and conduct obligations and, standards as well as the threat of enforcement action for failing to meet such obligations, particularly in relation to anti-money laundering/combating financing of terrorism (AML/CFT). However, there appear to be other factors at play too, including ethical, reputational and commercial considerations."[20]

– *JMLIT*

In the UK, there is a useful form of sharing intelligence between law enforcement and regulatory authorities on the one hand and the regulated sector on the other. Specifically, through the Joint Money Laundering Intelligence Taskforce (JMLIT) – a private-public partnership – regulated entities, the NCA and HM Revenue & Customs (HMRC) can sit around the table and discuss law enforcement and regulatory investigations and share intelligence – both ways – thanks to enabling legislation which allows for regulated entities to share sensitive information if the NCA is sitting at the table and requesting information. Though scientific evidence of impact is absent at present, such intelligence sharing is considered particularly valuable when it comes to targeting human trafficking, and it is becoming increasingly popular outside Europe, [21] though there are constitutional as well as cultural reservations in parts of Europe. There are also problems of scalability in both range of representation on JMLIT and the volume of reports that can be handled by such a body.

– *UK Government Plan of January 2019 to Reform the SAR Regime*

The UK Law Commission issued a report in 2018 proposing changes to the SAR regime. Notable proposals include modifications to the test of suspicion required for filing a SAR, allowing banks to process mixed criminal and legitimate funds in limited circumstances. The Commission also proposed the introduction of a corporate criminal offence of failure to ensure the reporting of

[20] David Artingstall, Nick Dove, John Howell, Michael Levi, "Drivers & Impacts of Derisking. A study of representative views and data in the UK", by John Howell & Co. Ltd. for the Financial Conduct Authority, February 2016, https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf.

[21] *Five years of growth in public–private financial information sharing partnerships to tackle crime*, RUSI, 2020.

suspected money laundering.[22] Its consultation paper highlighted that the low suspicion threshold for SAR filing combined with the individual criminal liability resulted in large-scale defensive (also known as precautionary) SAR filing. It was proposed that increasing the threshold to "reasonable grounds" would help reduce defensive SAR filing.[23]

In January 2019 the Home Secretary and Chancellor of the Exchequer announced that they would jointly chair the new Economic Crime Strategic Board, a taskforce that brings together representatives from the private sector (such as financial institutions), law enforcement agencies and regulatory bodies to tackle the economic crime threat. The Board meets biannually to set its priorities and direct its resources.[24] This model has been criticised by some NGOs, such as Global Witness and Corruption Watch, for including the major banks at its centre when, in their view, they are part of the problem.[25] (However, irrespective of that, banks are certainly part of the improvement – what 'the solution' would look like is uncertain to this author.)

It is yet to be seen to what degree the UK policymakers will adopt the recommendations made by the UK Law Commission, including the later report on Proceeds of Crime published 17 September 2020[26]. However, the Economic Crime Plan has been followed by a proposed Economic Crime Levy on *all* regulated persons above a low threshold, principally to fund the improvement of the SARs reporting infrastructure with £100 million.[27] This Levy is under active progress as I write, and its consultation period is now ended.

– *The Primary Criticisms of the FATF 2018 Mutual Evaluation Report*

The FATF has highlighted that the UK needs to strengthen the capacity and capabilities of the UK's FIU and the ability of the authorities to conduct systematic and strategic assessments of the UK money laundering threat. The limited role, resourcing and IT capacity of the FIU resulted in the FATF rating the overall effectiveness of UK financial intelligence regime as "moderate".

---

[22] "UK Law Commission Proposes Reforms to Suspicious Activity Reports for Money Laundering", Debevoise & Plimpton, 28 August 2018, https://www.debevoise.com/insights/publications/2018/08/uk-law-commission-considers-reforms-to-suspicious.

[23] https://www.nortonrosefulbright.com/en-gb/knowledge/publications/5ed49740/the-law-commission-consultation-on-reforming-the-sars-regime-key-takeaways-for-the-financial-sector

[24] "The law commission consultation on reforming the SARs regime: Key takeaways for the financial sector", Norton Rose Fulbright, August 2018, https://www.whitecase.com/publications/alert/sar-reform-case-causey-and-its-effect.

[25] "To all intents and purposes the [strategic board] is formalised policy capture of the economic crime agenda by precisely the corporations it ought to be policing": "Overhaul of financial crime rules too weak, warn critics", Financial Times, 12 July 2019, https://www.ft.com/content/0a4ed736-a400-11e9-974c-ad1c6ab5efd1.

[26] *Confiscation of the Proceeds of Crime after Conviction: A Consultation*, 2020.

[27] https://www.gov.uk/government/consultations/economic-crime-levy-consultation

Supervision of the legal and accounting sectors for AML and CTF purposes and the general understanding of financial-crime risks among professionals in these sectors was rated "moderate".

The report also highlighted the need to keep accurate and up-to-date the data in the beneficial shareholder public register (UK Companies House).

Those issues and the FIU's judged lack of autonomy from the NCA "in defining its role or its priorities," resulted in one of two "partially compliant" grades.

The UK pledged to increase the staff of the FIU, which it has done, though the average number of SARs per FIU member remains much the same. The UK government has considered long-pressed-for enhancements to the validity of the public register, and other changes, announced just prior to the 'FinCEN leaks' which revealed some serious failings in controls.[28]

Think tanks, NGOs, academia and members of the industry have noted that to justify its high ratings, they would have expected the UK to have achieved more. In particular, the UK remains a key destination for tainted funds. Some of the key shortcomings highlighted in UK's report, including issues with Companies House data and the inconsistent scrutiny into the real estate sector and certain professions (compared to scrutiny into banks) are viewed as significant. As Tom Keatinge of RUSI observed:

> "The UK has achieved top-of-the-class marks from the FATF – government officials will be both surprised and relieved. However, the fact that the UK remains central to global money laundering schemes brings into question the relevance of this evaluation. Furthermore, we have cause to question some of the findings in the report, in particular, the assessment in relation to the effective use of financial intelligence by UK law enforcement."[29]

II. AIMS AND SCOPE OF AML SYSTEMS

AIMS OF THE AML/CTF REGIME

Generally, the language used in legislation implies that the AML/CTF regime aims to prevent the corruption and misuse of the financial system for the purposes of money laundering and the furthering of crime (including terrorism). More specifically, the Money Laundering Regulations state in the introductory part that they transpose the EU Directive on the prevention of the use of

[28] https://www.gov.uk/government/consultations/corporate-transparency-and-register-reform; https://www.gov.uk/government/news/reforms-to-companies-house-to-clamp-down-on-fraud-and-give-businesses-greater-confidence-in-transactions.

[29] "RUSI Experts React to UK's Financial Action Task Force Mutual Evaluation Report", RUSI, 7 December 2018, https://rusi.org/rusi-news/rusi-experts-react-uk-financial-action-task-force-mutual-evaluation-report.

the financial system for the purposes of money laundering and terrorist financing: the phrase "prevention of the use of the financial system for the purposes of money laundering or terrorist financing" is reiterated multiple times throughout the regulations.

However, a key and direct objective is to help confiscate the assets of criminals, and prevent criminals from enjoying them.[30] The key AML piece of legislation is POCA, amended subsequently and supported by the Money Laundering Regulations of 2017 (previously of 2007) and 2019. This law aims at supporting the confiscation of crime proceeds, including through civil recovery channels. The Assets Recovery Agency was subsequently abolished because of its failure to confiscate funds in excess of its costs. Its civil recovery functions were subsumed into SOCA (now the NCA), and have not been utilised extensively since then. There have been significant successes in using POCA powers to recover criminal assets,[31] with:

- £1.6 billion being recovered from criminals between April 2010 and March 2018
- over £180m has been paid in compensation to victims from confiscation between 2012/13 and 2017/18, with £30m paid in 2017/18, and
- hundreds of millions more have been frozen and – to adapt the phraseology of disarmament in the Good Friday Agreement – 'put beyond criminal use'. For example, Account Freezing Orders (AFOs) were introduced in the Criminal Finances Act 2017 (CFA) and were used more than 650 times in 2018/19 to freeze over £110m of suspected illicit funds, an unknown proportion of which will eventually be confiscated.

As the POCA section of the website of the CPS[32] notes:

> "Therefore, where there is sufficient evidence to meet the evidential test under the Code for Crown Prosecutors, the following Public Interest factors in favour of prosecution for offences of money laundering should be very carefully considered:
> – The importance of making it more difficult for criminals to legitimise their ill-gotten gains;
> – The importance of deterring professional launderers;
> – The importance of protecting the integrity of financial institutions domestically and internationally."

[30] In the UK's Serious and Organised Crime Strategy 2018, the Home Secretary notes (p. 2): "Our revised approach puts greater focus on the most dangerous offenders and the highest harm networks. Denying perpetrators the opportunity to do harm and going after criminal finances and assets will be key to this." The first objective of the strategy states (p. 6): "We will use new and improved powers and capabilities to identify, freeze, seize or otherwise deny criminals access to their finances, assets and infrastructure, at home and overseas including Unexplained Wealth Orders and Serious Crime Prevention Orders."

[31] HMG Asset Recovery Action Plan 2019

[32] https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences.

SCOPE OF MONEY LAUNDERING

1. *Definition of Money Laundering in Criminal Law*

a. *Actus reus*

i. PREDICATE OFFENCES

Under POCA, the Crown has to prove that the laundered proceeds are "criminal property", as defined in section 340 POCA: that is to say that the property constitutes a person's *benefit* from *criminal conduct* (whether via a criminal prosecution or a civil recovery path under which evidence has only to meet the balance of probabilities test).

"Criminal conduct" is all conduct which constitutes an offence in any part of the UK (which means that an "all crimes" approach is adopted in respect of predicate crimes committed in the UK)..[33]

Under POCA, any criminal conduct which generates proceeds or other economic benefit (e.g. criminal tax savings) can be considered a predicate offence regardless of whether it has occurred in the UK or abroad, subject to the condition that if it had had occurred abroad, even if lawful in that country at the time it occurred, it had to be a criminal offence in the UK and punishable (in principle) by more than a year of imprisonment.

ii. DEFINITION OF MONEY LAUNDERING ACTS

In short, POCA describes the money laundering offences as follows:

- A person commits an offence if he conceals, disguises, converts, or transfers criminal property, or removes criminal property from England and Wales, Scotland or Northern Ireland. Concealing or disguising criminal property includes concealing or disguising its nature, source, location, disposition, movement, ownership or any rights connected with it.
- A person commits an offence if he enters into, or becomes concerned in an arrangement which he knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person.
- A person commits an offence if he acquires, uses or has possession of criminal property: this includes the proceeds of his own crimes.

[33] Ibid. In some cases there is extra-territorial jurisdiction, most notably the Bribery Act 2010.

Under POCA, prosecutors have to prove that the laundered proceeds are "criminal property", as defined in section 340 POCA: that is to say that the property constitutes a person's benefit from criminal conduct.

There is no certainty in regards to how commingled property (i.e. legitimate and illegitimate) should be treated. The general understanding of the law is that dealing with mixed funds can give rise to criminal liability. There have been multiple instances of financial institutions in the UK being fined for weakness in their AML systems and controls. From a disclosure perspective, it is irrelevant whether the funds are solely of criminal origin or mixed. Regulators do not even have to prove that there are crime proceeds at all if they see what they define as a "weakness" (which can be broadly interpreted to include a range of issues), though this can lead to remedial action rather than a formal penalty under the discretionary model. The Law Commission proposed in 2018 changes to the SAR regime to raise the reporting threshold and allow, within limited circumstances, dealing with mixed funds. Prosecutions are not the only index of seriousness or of effectiveness, but an article in the FCPA blog in March 2018 highlighted that, "[d]espite the UK's rhetoric about wanting a 'world leading reputation for integrity' as a financial center, it has never prosecuted a single company or bank for money laundering."[34] As the Law Commission noted in their 2018 consultation paper, in the absence of significant case law, the broadly drafted legislation combined with inconsistent sector-specific guidance makes it difficult for obliged entities to understand their obligations.[35]

Where the illegitimate property/funds/benefit cannot be ring-fenced, value-based (as opposed to object-based) confiscation may be pursued, which in any event has always been the UK model other than for cash and instrumentalities of crime forfeiture. In such instances, the equivalent of what is believed to be the illegitimate portion of the commingled property will be subject to confiscation. (The authorities can seize the cash and, unless a licit origin is demonstrated, can confiscate it.)

As explained in a 2017 UNODC report, in the UK

> "default of payment of a value based confiscation order can result in an additional period of imprisonment being levied. The convicted person may however apply for a reduction in the value of the order if he or she can show that they have no other assets from which to pay. If the convicted person refuses to pay or claims he or she has no assets from which to pay, apart from an additional

[34] Susan Hawley, "The UK doesn't prosecute money laundering (and that should change)", FCPA blog, 20 March 2018, http://www.fcpablog.com/blog/2018/3/20/susan-hawley-the-uk-doesnt-prosecute-money-laundering-and-th.html.

[35] "The law commission consultation on reforming the SARs regime: Key takeaways for the financial sector", Norton Rose Fulbright, August 2018, https://www.nortonrosefulbright.com/en-gb/knowledge/publications/5ed49740/the-law-commission-consultation-on-reforming-the-sars-regime-key-takeaways-for-the-financial-sector.

period of imprisonment being levied, the following enforcement mechanism are typically available for the collection of unfulfilled value based confiscation orders.

- The confiscation order has the status of a civil judgment and the government becomes a judgment creditor. The debt can be collected through ordinary civil law enforcement mechanisms, such as insolvency/bankruptcy proceedings; or
- Special realisation procedures are provided for as part of the asset recovery law."[36]

Tax evasion is a predicate offence to money laundering. In *R v Allen*, the Court decided that a person who "benefits" from tax evasion benefits to the extent of the tax evaded, although scholars have noted that this is not straightforward.[37] Given that tax evasion is a predicate offence, but one that generates illegal savings as opposed to profit in the ordinary sense of that word, and given that mixed funds give rise to liability, it is unclear where a line should be drawn and whether funds should be treated differently for the tax evasion charges as opposed to the money laundering charges.[38]

b. *Mens rea*

Knowledge or suspicion that the property is of criminal origin is an essential requirement for liability and, therefore, the *mens rea*, under each of the principal money laundering offences under POCA sections 327, 328 and 329.

The Court of Appeal has held that the meaning of "suspicion" under the Criminal Justice Act 1988 (the predecessor of POCA) is that "the defendant must have thought that there was a possibility, which was more than fanciful, that the other person was or had been engaged in or had benefited from criminal conduct. A vague feeling of unease would not suffice. This is subject, in an appropriate case, to the further requirement that the suspicion so formed should be of a settled nature".[39] The same meaning is to be adopted in civil proceedings that arise out of the

---

[36] Study prepared by the Secretariat on effective management and disposal of seized and confiscated assets, Open-ended Intergovernmental Working Group on Asset Recovery, UNODC, 23 August 2017, https://www.unodc.org/documents/treaties/UNCAC/WorkingGroups/workinggroup2/2017-August-24-25/V1705952e.pdf.

[37] *R v Allen* [2001] UKHL 45; Peter Alldridge, "Smuggling, Confiscation and Forfeiture", *The Modern Law Review*, 65(5) (2002) 781–791.

[38] "The wide definition of criminal property may result in a relatively small amount of criminal property tainting a significantly larger asset […] in cases of tax evasion, failure to declare turnover upon which tax should be paid generally renders the entire turnover criminal property" SARs Regime Good Practice Frequently Asked Questions Defence Against Money Laundering (DAML), NCA, May 2019, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/167-defence-against-money-laundering-daml-faq-may-2018/file#:~:text=A%20DAML%20does%20not%20provide,of%20the%20funds%20in%20question.

[39] *R v Da Silva* [2006] EWCA Crim 1654, although in *Shah and another v HSBC Private Bank (UK) Ltd [2012] EWHC 1283* the judge ruled that this formulation ("of a settled nature") is only applicable in limited circumstances (see https://www.bclplaw.com/en-GB/thought-leadership/landmark-decision-in-shah-v-hsbc-private-bank-brings-welcome-relief-for-firms.html).

money laundering provisions under Part 7 of the POCA.[40] There is no requirement for suspicion to be reasonable.[41] It is not necessary to know the precise details of the predicate offence and prosecutors do not have to prove the predicate offence at the criminal law standard. In fact, they do not need to know what type of predicate offence generated the proceeds.

2. *Money Laundering by Omission*

It is commonly understood that there is criminal liability if the omission is the result of gross negligence, akin to recklessness,[42] or deliberate non-disclosure rather than the result of money laundering being impossible to detect within the due process that the regulated sector can reasonably put in place. The Money Laundering Regulations require that regulated entities and regulated professionals undertake due diligence on customers to confirm their bona fides. Section 331 POCA creates an offence of failure to disclose in respect of nominated officers (i.e. compliance officers) in the regulated sector who receive disclosures based under section 330 and who do not pass the information to the FIU as the disclosure-receiving unit when they:

- know or suspect; or
- have reasonable grounds for knowing or suspecting that another person is engaged in money laundering.[43]

However, when it comes to mere negligence (as opposed to gross negligence), there are different schools of thought.

One school of thought argues that POCA effectively criminalises negligence in the regulated sector.[44] In particular, section 330(3) POCA states: "The second condition is that the information or other matter – (a) on which his knowledge or suspicion is based, or (b) which gives reasonable grounds for such knowledge or suspicion, came to him in the course of a business in the regulated sector."

Lawyers have highlighted:

---

[40] *K Ltd v National Westminster Bank Plc* [2007] 1 WLR 311.

[41] Paul Marshal, Chancery Bar Association, Money Laundering Explanatory Note, Part 1, Substantive Law, May 2013.

[42] In the law of England and Wales, recklessness may be defined as the conscious taking of an unjustified risk. Negligence is unreasonable conduct that creates risk, while gross negligence is a high degree of negligence that may deserve criminal punishment. In *R v G & R* [2003] UKHL 50, it was determined that recklessness was punishable criminally where: (i) a circumstance when he is aware of a risk that it exists or will exist; (ii) a result when he is aware of a risk that it will occur; and it is, in the circumstances known to him, unreasonable to take the risk.

[43] See https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences.

[44] Outside of the regulated sector this offence cannot be committed by negligence. See https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences.

> "The consensus of the learned authors of Archbold (2018) and of the leading specialist textbook 'Mitchell, Taylor and Talbot on Proceeds of Crime' (which is reproduced in the CPS's legal guidance) is that subsection 330(2)(b) is an offence committed by negligence. Archbold instructs its readers that section 330 (and section 331) 'introduce a negligence test.' Accordingly, a person may commit an offence under it 'even if he did not actually know or suspect' (para 26-22). The latter textbook endorses this interpretation: 'The offence is committed by a person who has the necessary knowledge or suspicion but also where, in the circumstances, he should at least have suspected that the other person was engaged in money laundering.'"[45]

It can be argued that policymakers have deliberately included the "reasonable grounds" provision to enforce the expectation that firms and professionals in the regulated sector follow a process, which includes Know-Your-Customer (KYC) and due diligence checks and transactions monitoring, in finding out whether there are reasonable grounds to suspect the property is of criminal origin. If firms and professionals are able to demonstrate they have followed an appropriate process and have taken all reasonable steps, then they can claim that defence. Section 331 POCA, as well the availability of the aforementioned defence, do not depend on whether money laundering is actually taking place or has ever taken place.

The 'reasonable grounds" provision does not apply outside the regulated sector, according to POCA. Additionally, the CPS explicitly states that the offence of failure to disclose by nominated officers outside the regulated sector (section 332 POCA) cannot be committed by negligence. The mental element of this offence is knowledge or suspicion.[46] This supports the argument that nominated officers in the regulated sector, in theory, may be prosecuted for negligence.

As there is significant scope for interpretation as to what appropriate process should entail, the regulated sector may not find it easy to persuade regulators to concur with their assessment, though regulators may be unable to show how to detect money laundering in those circumstances. Nominated officers in the regulated sector facing liability are fearful, leading to significant defensive SAR reporting (as highlighted by the Law Commission) and de-risking of individual and business clients whose conduct may attract the wrath of regulators. While there are reported sentencing cases under subsection 330(2)(a), there is no jurisprudence yet concerning subsection 330(2)(b).

If it is expected that information will "come to" the nominated officer if he has ensured adequate anti-financial crime processes, controls and supervision, then the question is whether failure to o 'correctly assess' this information constitutes negligence. This is perhaps where a line can be drawn between, on the one hand, negligently ignoring information and the need for adequate

[45] David Corker, "Failure to disclose does not equate to negligence", Corker Binning blog, 7 February 2018, https://www.corkerbinning.com/failure-to-disclose-does-not-equate-to-negligence/

[46] https://www.cps.gov.uk/legal-guidance/proceeds-crime-act-2002-part-7-money-laundering-offences.

processes, and, on the other, making a genuine error in judgment when assessing the information. It would seem to make sense that at least in the latter case, prosecutors will have to prove beyond reasonable doubt that the nominated officer knew, suspected or had – in the sense of understanding – reasonable grounds to know or suspect. But more criminal trials and perhaps sentencing are required for there to be certainty about this. A conviction for the primary money laundering offences carries a maximum punishment of imprisonment for 14 years or a fine or both. The secondary offence of failure to disclose carries a maximum punishment of five years.[47]

As so often, however, it is difficult to translate these theoretical liabilities into practice. The UK Financial Conduct Authority has discontinued half of its criminal investigations into breaches of the money laundering rules since January 2020, and is yet to bring a single prosecution — despite a pledge to make full use of its powers. In the first 8 months of 2020, seven out of 14 criminal investigations into contraventions of the money laundering regulations have been shut down by it. Five of these were "single track", or solely criminal, probes, while the other two were "dual track" investigations that could have resulted in either criminal or civil proceedings. As a result of these decisions, only one single-track criminal investigation is still being pursued — the other six are dual track and may result only in civil outcomes, though at present it is too early to tell.[48]

3. Aggravated Form of Money Laundering

An individual found guilty of one of the primary offences (sections 327–329) is liable to a maximum term of imprisonment of 14 years and an unlimited fine, if sentenced in a Crown Court. Beyond this, the law does not define in detail what an aggravated form of money laundering is, but the courts would decide through case law – influenced by Sentencing Council guidelines[49] – in what instances higher sentences in the range of 14 years' imprisonment should be imposed. There are no extra powers for the more serious end of the spectrum cases, but these may sometimes be sought after for their publicity and associated both special and general deterrent value.

4. Statutes of Limitation

As is common in UK legislation, no limitation period applies to money laundering and terrorist financing offences committed under POCA. (Offences committed before POCA came into force are subject to previous legislation, but these are unlikely now to be prosecuted 17 years later.)

---

[47] Ibid.

[48] 'FCA scraps half its criminal probes into money-laundering breaches', *Financial Times,* 14 September 2020.

[49] *Fraud, Bribery and Money Laundering Offences: Definitive Guideline*, Sentencing Council, 2014.

However, the principal/primary money laundering offences under POCA are subject to a defence of assumed consent where a SAR is made to the authorities and, if consent is refused during the seven working days' notice period, a moratorium period has elapsed. The moratorium is 31 days, but under the Criminal Finances Act 2017 a senior officer will be able to apply to the Crown Court to increase the moratorium in up to 31-day increments, up to a total of 217 days.[50] Consent is requested where there is a pending transaction (i.e. in only some types of relationships/products will a consent be needed). This pending transaction cannot lawfully be executed in the 31 days.

5. *Jurisdictional Rules*

In short, both for some predicate offences and for money laundering, there is extraterritorial effect that the courts can pursue if there are harmful consequences in the UK.

Under POCA, any criminal conduct which generates proceeds or other economic benefit can be considered a predicate offence regardless of whether it has occurred in the UK or abroad, subject to the condition that if it had had occurred abroad and, even if not unlawful in that country at the time it occurred, it was criminal in the UK and punishable (in principle) by more than a year of imprisonment. The CPS notes, however, that the laundering act must have occurred within the UK jurisdiction.[51]

In other words, for conduct punishable by less than a year of imprisonment, there is an exception to the extraterritorial reach described as the "overseas conduct defence". A person will not be liable under sections 327–329 if:

- he or she knew or reasonably believed that the relevant criminal conduct occurred abroad; and
- that relevant criminal conduct was not, when it took place, unlawful under the criminal law of that other country.

The "overseas conduct defence" does not apply to conduct that (despite being legal under local law) would constitute an offence punishable by a maximum sentence of imprisonment over 12

[50] BCL Solicitors LLP, "Anti-money laundering and fraud in the United Kingdom", Lexology, 28 December 2018, https://www.lexology.com/library/detail.aspx?g=f0870ad8-910f-4bef-a6f3-5445c93bd94d; "Criminal Finances Act 2017 provisions to come into force tomorrow", Herbert Smith Freehills, 30 October 2017, https://hsfnotes.com/fsrandcorpcrime/2017/10/30/criminal-finances-act-2017-provisions-to-come-into-force-tomorrow/.

[51] "For the purpose of Part 7 the Proceeds of Crime Act 2002, offences which were committed abroad are relevant predicate crimes if laundering acts are committed within our jurisdiction where the predicate offence committed abroad (from which proceeds were generated) would also constitute an offence in any part of the United Kingdom if it occurred here (section 340 (2)(b)) (see Archbold)." See: https://www.cps.gov.uk/legal-guidance/jurisdiction.

months in the UK if it had occurred in the UK. Hence there are very few offences to which the defence applies.

There is scope for interpretation as to what extent the primary money laundering offences under POCA (see section II.B.1.a.ii) have extraterritorial jurisdiction. However, through case law the courts have stipulated that the UK jurisdiction can extend to money laundering conduct abroad and that the language in POCA indicated that Parliament had intended for the Part 7 offences to be extraterritorial in effect. In *R v Rogers & ors*,[52] the Court of Appeal of England and Wales held that the three money laundering offences in Part 7 POCA have extraterritorial effect, such that an offence of converting criminal property under section 327(1)(c) POCA could be tried in the UK even where the defendant, who lived and worked in Spain, committed no part of the offence within the UK.[53] This is because the conduct's harmful consequences – i.e. a significant measure of the criminal conduct – took place in the UK.

NON-CRIMINAL DEFINITION OF MONEY LAUNDERING

The legal system in the UK uses one definition of money laundering which is based on the definition of money laundering in the EU directives.

SCOPE OF OBLIGED ENTITIES

The obliged entities which form the regulated sector are:

- credit institutions (banks, building societies, others);
- financial institutions; Money Service Businesses; electronic money institutions; auction platforms; recognised investment exchanges; payment service providers;
- auditors, insolvency practitioners, external accountants and tax advisers;
- independent legal professionals;[54]
- trust or company service providers;
- estate agents and letting agents;
- high-value dealers;[55]
- casinos;

[52] [2014] EWCA Crim 1680.

[53] See for more details: "Money laundering offences apply to conduct occurring entirely outside the UK", Allen& Overy, 20 April 2015, http://www.allenovery.com/publications/en-gb/Pages/Money-laundering-offences-apply-to-conduct-occurring-entirely-outside-the-UK.aspx.

[54] Independent legal professionals include firms or sole practitioners that provide, by way of business, legal or notarial services to other people, for instance when participating in financial or real property transactions.

[55] A high-value dealer under Money Laundering Regulations is any business or sole trader that accepts or makes high-value cash payments of €10,000 or more (or equivalent in any currency) in exchange for goods.

- art market participants;
- cryptoasset exchange providers;
- custodian wallet providers.

Every business covered by the Money Laundering Regulations must be monitored by a supervisory authority. A large part of the financial institutions and financial services providers, such as banks, are supervised by the FCA.

According to the Money Laundering Regulations:

> "7.—(1) Subject to paragraph (2), the following bodies are supervisory authorities—
> (a) the FCA is the supervisory authority for—
> (i) credit and financial institutions which are authorised persons but not excluded money service businesses;
> (ii) trust or company service providers which are authorised persons;
> (iii) Annex 1 financial institutions;
> (iv) electronic money institutions;
> (v) auction platforms;
> (vi) credit unions in Northern Ireland;
> (vii) recognised investment exchanges within the meaning of section 285 of FSMA(b);
> (viii) cryptoasset exchange providers;
> (ix) custodian wallet providers
> (b) each of the professional bodies listed in Schedule 1 is the supervisory authority for relevant persons who are regulated by it;
> (c) the Commissioners for Her Majesty's Revenue and Customs are the supervisory authority for—
> (i) high value dealers;
> (ii) money service businesses which are not supervised by the FCA;
> (iii) trust or company service providers which are not supervised by the FCA or one of the professional bodies listed in Schedule 1;
> (iv) auditors, external accountants, insolvency practitioners, tax advisers and independent legal professionals who are not supervised by one of the professional bodies listed in Schedule 1;
> (v) bill payment service providers which are not supervised by the FCA;
> (vi) telecommunication, digital and IT payment service providers which are not supervised by the FCA;
> (vii) estate agents who are not supervised by one of the professional bodies listed in Schedule 1;
> (viii) art market participants;
> (d) the Gambling Commission is the supervisory authority for casinos.
> (2) Where under paragraph (1) there is more than one supervisory authority for a relevant person, the supervisory authorities may agree that one of them will act as the supervisory authority for that person.

Telecommunications, digital and IT payment service providers are considered obliged entities as providers of payment services."

A range of professional services regulated by their own professions (see (b) above, referring to Schedule 1, self-regulatory organisations[56]) – 22 Professional Body Supervisors (PBSs) responsible for AML supervision for the accounting and legal sectors – are under the meta-supervision of OPBAS (the Office for Professional Body Anti-Money Laundering Supervision), a regulator set up in 2018 by the government to try to ensure that these 22 AML supervisors provide consistently high standards of AML supervision set out in the Money Laundering Regulations.[57] OPBAS is housed at the FCA. It is likely that OPBAS will try to merge some of these disparate bodies, but whether this will lead to consistent supervision is an open question.

Financial and Banking Institutions

Credit institutions (banks, building societies, others) and financial institutions (Money Service Businesses and others) are among the obliged entities.

6. Virtual Currency System Participants

Virtual currency system participants are not yet regulated. There is a plan for self-regulation, but it is unclear at this stage how this will progress.

If a virtual currency system is also deemed to be a financial institution, then it will be regulated by either the FCA or HMRC (or both) and will be covered by the Money Laundering Regulations. See also section I.A. for 2019 amendments to the regulations in regard to cryptoasset exchange providers.

7. Legal Profession and Tax Advisors

These are covered by the Money Laundering Regulations regardless of the nature of activity they perform (e.g. financial intermediation, setting up companies and so on). However, their

[56] The Association of Accounting Technicians; the Association of Chartered Certified Accountants; the Association of International Accountants; the Association of Taxation Technicians; the Chartered Institute of Legal Executives/CILEx Regulation; the Chartered Institute of Management Accountants; the Chartered Institute of Taxation; the Council for Licensed Conveyancers; the Faculty of Advocates; the Faculty Office of the Archbishop of Canterbury; the General Council of the Bar/Bar Standards Board; the General Council of the Bar of Northern Ireland; the Insolvency Practitioners Association; the Institute of Certified Bookkeepers; the Institute of Chartered Accountants in England and Wales; the Institute of Chartered Accountants in Ireland; the Institute of Chartered Accountants of Scotland; the Institute of Financial Accountants; the International Association of Bookkeepers; the Law Society/Solicitors Regulation Authority; the Law Society of Northern Ireland; and the Law Society of Scotland. See http://www.legislation.gov.uk/uksi/2017/692/schedule/1/made.

[57] https://www.fca.org.uk/opbas. See Schedule 1 Money Laundering Regulations.

obligations and criminal law risks are affected by whether they are performing these acts as part of the regulated sector or not.

8. *Informal Value Transfer Systems*

Informal value transfer systems are not part of the AML regulated sector. If such providers are informal, i.e. not registered as such, they may be unknown to the authorities, though it is an offence to supply financial services without being registered. However, if they agree to comply with the Money Laundering Regulations and register (at a cost)[58] with HMRC, they will be regulated for AML purposes.

9. *Non-profit Sector*

NGOs and charities are not covered by the Money Laundering Regulations, although the NCA's annual SAR reports indicate that there is a certain percentage of SARs filed by charities. Charities are required by their own sector oversight body – the Charity Commission – to report suspicious activity.[59] The Charity Commission has the power to strike them (and individual trustees) off if they violate the criteria, including failing to have adequate standards of identification of where money goes to. There is particular concern about terrorism finance risks in the charity sector.

According to the UK government,[60] services that are provided by certain charities and public sector bodies are not covered by the Money Laundering Regulations. This is because the services

[58] https://www.gov.uk/guidance/money-laundering-regulations-registration-fees

[59] https://www.charitycommissionni.org.uk/charity-essentials/controlling-against-terrorist-financing-and-money-laundering/. Of course, where those running the charity are also engaged in crime, this is unlikely. The most recent public case is the Orthodox Jewish charity network which had an "enormous jump" in income in 2012 to £8 million, having recorded an annual income of £1.7 million between 2008 and 2011, due to sales of counterfeit Viagra and allied products. The principal was sentenced to seven and a half years' imprisonment in 2019 (though he fled while on bail), and only then was the Charity Commission able to announce its investigation. The case appears to have been launched after customers complained the online-purchased drugs did not work, and the investigators discovered large numbers of online card payments to the charities' accounts. See Isabella Nikolic, "Money launderer, 67, who tried to buy a knighthood is convicted in his absence of £10million Jewish charities scam after going on the run", Daily Mail, 24 June 2019, https://www.dailymail.co.uk/news/article-7174919/Money-launderer-67-convicted-10million-Jewish-charities-scam-going-run.html; Emma Bartholomew, "Stamford Hill Orthodox Jewish charity finance boss laundered £10m through selling 'dangerous' fake Viagra and diet pills", Hackney Gazette, 10 July 2019, https://www.hackneygazette.co.uk/news/crime-court/charities-laundered-10m-through-fake-viagra-sales-1-6153522. It allegedly warned Medical Aid for Palestinians to be careful that it did not distribute funds inappropriately, following a complaint by Jewish organisations, but took no formal action: Zachary Keyser, "Charity Commission Warns Medical Aid for Palestinians about Funding Misuse", Jerusalem Post, 25 March 2019, https://www.jpost.com/Middle-East/Charity-Commission-warns-Medical-Aid-for-Palestinians-about-funding-misuse-581860.

[60] https://www.gov.uk/guidance/money-laundering-regulations-who-needs-to-register#charities-and-public-sector-bodies. See also https://www.charitycommissionni.org.uk/charity-essentials/controlling-against-terrorist-financing-and-money-laundering/.

are not carried out 'by way of business'. There are tightly drawn types of charity and public body that do not have to register with HMRC under the Money Laundering Regulations.

RELATIONSHIP BETWEEN AML AND ANTI-TERRORISM FINANCING FRAMEWORK(S)

SARs relating to terrorist financing are submitted to the UK's FIU under the Terrorism Act 2000.[61] The preventive regime is currently combined (in the aftermath of 9/11) and the regulated sector has to have an anti-financial crime programme that covers terrorist financing risk alongside money laundering risk. But the UK's FIU separates the terrorist financing-related SARs from the rest of the SARs and has a dedicated specialist team reviewing them. Terrorism-related SARs are disseminated to the National Terrorist Financial Investigation Unit (part of the Metropolitan Police Service Counter Terrorism Command) and other counterterrorism-related agencies. Additionally, under the "consent"/"defence" regime , where the consent request has been refused under the Terrorism Act, there is no moratorium period, and there is no defence unless and until the request is granted by the NCA. Other than that, there are no formal and material differences between the AML and counter-terrorist financing regimes.

While there is the acknowledgement that in terrorist financing amounts are often small and may come from licit as well as illegal sources, there is hardly any notable debate about how these phenomena should be treated differently by practitioners, regulators or regulated entities. It could be argued that in practice, the (politically and socially) acceptable risk level in terrorist financing is zero (perhaps especially because of universal risks from US civil claims on behalf of American victims). But there is an ongoing discussion about how the perception that charities are high risk from a terrorist financing perspective harms the charitable sector in the UK.

As the UK Charity Commission's chairman William Shawcross has asserted, "terrorist abuse is one of the greatest risks facing the charitable sector today"[62] as it seriously undermines public confidence in providing humanitarian aid. (Though this preceded the scandals involving major charities' suppression of scandals involving staff engaged in sexual oppression in overseas operations, it may remain the Commission's view today.) However, as noted recently by UK authorities, de-risking by withdrawing bank services to charities may mean "charitable funds may go underground, increasingly transacted in cash, or moved off-shore via cash couriers or alternative remittance systems."[63]

[61] There have been amendments/enhancements to the Act since 2000.
[62] Andrew Gilligan, "'Terror link' charities get British millions in Gift Aid", Daily Telegraph, 29 November 2014.
[63] HM Treasury and Home Office, *UK national risk assessment of money laundering and terrorist financing*, October 2015.

III. THE SYSTEM OF MONEY LAUNDERING PREVENTION

CUSTOMER DUE DILIGENCE

1. Standard CDD Rules

a. Triggers and Timing

According to the Money Laundering Regulations and the JMLSG,[64] an obliged entity/obliged professional must apply CDD measures when it does any of the following:

- establishes a business relationship;
- carries out an occasional transaction;
- suspects money laundering or terrorist financing; or
- doubts the veracity of documents or information previously obtained for the purpose of identification or verification.[65]

The above applies to all types of obliged entities.

According to the Money Laundering Regulations, an "occasional transaction" for CDD purposes means:

- a transfer of funds within the meaning of article 3.925 of the Funds Transfer Regulation exceeding €1,000; or
- a transaction carried out other than in the course of a business relationship (e.g. a single foreign currency transaction, or an isolated instruction to purchase shares), amounting to €15,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

A casino must also apply customer due diligence measures in relation to any transaction amounting to €2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

A letting agent must also apply customer due diligence measures in relation to any transaction which consists of the conclusion of an agreement for the letting of land.

---

[64] The JMLSG is made up of the leading UK Trade Associations in the Financial Services Industry (http://www.jmlsg.org.uk/), which themselves have undergone some rationalisation under the banner of UK Finance. It produces guidance for firms in the financial services sector, most notably banks. This guidance must be approved by the Treasury. The most recent guidance – approved August 2020 – is available at https://jmlsg.org.uk/guidance/current-guidance/.

[65] For more details see JMLSG, Regulation 27(1), 5.2.1, http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current.

An art market participant must also apply customer due diligence measures—

(a) in relation to the trade of a work of art when the firm or sole practitioner carries out, or acts in respect of, any such transaction, or series of linked transactions, whose value amounts to €10,000 or more;

(b) in relation to the storage of a work of art, when it is the operator of a freeport and the value of the works of art so stored for a person, or series of linked persons, amounts to €10,000 or more.

A cryptoasset exchange provider of the kind who operates a machine which utilises automated processes to exchange cryptoassets for money, or money for cryptoassets, must also apply customer due diligence measures in relation to any such transaction carried out using that machine.

b. CDD Measures

UK regulators do not take a prescriptive approach and expect the regulated sector to take a risk-based approach and decide what measures to take depending on the level of risk (though all over the world, 'risk' in an AML context is seldom based on serious analytical evidence). Separate guidance has been issued to the regulated sector by the relevant industry associations or supervisory bodies. It does not necessarily matter in which part of the regulated sector the obliged entity operates; rather, what matters is the size and complexity of the entity's business and the risks it faces along a range of dimensions.

c. Individual Responsibility

According to 2017 changes in the Money Laundering Regulations, obliged entities must now appoint a money laundering compliance principal (MLCP) and that individual must be on the board of directors (or equivalent management body), or a member of senior management, where appropriate to the size and nature of the business. Essentially this aims to ensure that responsibility rests with the board as well as with the money laundering reporting officer (MLRO) and it is in the interest of the board to fully understand the financial crime risks their organisation faces and how these are mitigated. MLCPs do not get involved in the day-to-day decision making as to whether to file a SAR and how to conduct investigations. They take part in the more strategic decisions such as defining the organisation's risk appetite. It is theoretically possible (and indeed is intended) that this upwards 'responsibilisation' of the Board of Directors may increase the risks of corporate criminal liability, which in the UK is dependent on being able to prove that the acts were at the behest of the 'directing mind' of the corporation. However, there are no cases where prosecutions have occurred on this basis.

d. Further CDD Guidance

Various bodies provide guidance to the various parts of the regulated sector (e.g. accountancy, legal sector, financial services).

For instance, for audit, accountancy, tax advisory, accountancy-related services firms and trust and company services firms guidance on how to help prevent money laundering and terrorist financing has been produced by the Consultative Committee of Accountancy Bodies and is based on law and regulations as of January 2020.[66] This guidance has to be approved by HM Treasury in order to be published as final. Among other things, the guidance explains what the concept of a "risk-based approach" means, how to assess risk, and what CDD is, in what situations it is required and what it entails; it also discusses suspicious activity reporting, record keeping, and training and awareness.

Similarly, the various iterations of the guidance produced by the JMLSG undergo a process of approval by the HM Treasury.

The FCA Handbook also contains guidance relevant to FCA-regulated firms.

The AML/counter-terrorist financing guidance produced by the legal sector AML supervisors, including the Law Society, in March 2018, has also received the approval of HM Treasury,[67] and is currently awaiting approval (September 2020).

The various pieces of guidance are not dissimilar from each other in approach and concepts. The provisions in respect of lawyers will be discussed in a separate document.

2. Simplified CDD

a. Scope

Before the 4AMLD was transposed into national legislation through the 2017 regulations (Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017), simplified due diligence was commonly applied automatically in cases of regulated and/or listed companies, particularly in "lower-risk" jurisdictions (as judged by the FATF and the international consensus, whether analytically justified or not). With the 2017 change in regulations, simplified CDD can now be applied by any obliged entity *only* upon appropriate risk assessment to evidence that the client subject to due diligence is low risk. The risk assessment

[66] https://www.ccab.org.uk/wp-content/uploads/2020/09/AMLGuidance2020.pdf.

[67] Law Society, "Anti-money laundering guidance", 6 March 2018, https://www.lawsociety.org.uk/policy-campaigns/articles/anti-money-laundering-guidance/.

should include looking at geography risk, industry risk and risk associated with the product and delivery channels.

b. Requirements

UK legislation and relevant guidance do not prescribe the exact steps that customer due diligence and simplified due diligence have to entail.

According to the JMLSG guidance, simplified due diligence means not having to apply CDD measures, but this is only in the aftermath of 'adequate' risk assessment that can demonstrate that risk is low. In practice, this means not having to verify the customer's identity, or, where relevant, that of a beneficial owner, nor having to obtain information on the purpose or intended nature of the business relationship, although there is some scope for interpretation. It is, however, still necessary to conduct ongoing monitoring of the business relationship to show that the risk is not raised by a subsequent change in account behaviour. Firms must have reasonable grounds for believing that the customer, transaction or product relating to such transaction falls within one of the categories set out in the Regulations, and may have to demonstrate this to their supervisory authority. Clearly, for operating purposes, the firm will nevertheless need to maintain a base of information about the customer.

There is no material difference between how simplified due diligence is applied by the different types of obliged entities. However, it can be inferred from legislation that certain businesses, when offering certain products (e.g. a life insurance policy for which the premium is low; see criteria in the Money Laundering Regulations 2017 and 2019), typically face lower risk of money laundering and therefore can take simplified measures.

c. Further Simplified CDD Guidance

As discussed above, guidance is provided by various industry bodies (e.g. JMLSG) but needs to be approved by HM Treasury. The FCA also issues guidance to those firms that are FCA-regulated. As discussed in the section above, legislation and guidance indicate that simplified CDD means that certain CDD measures do not need to be taken. But basic identification and monitoring of the relationship are still required. The approach in the UK is not to provide prescriptive guidance: so obliged entities decide at their own discretion what exactly the various levels of due diligence would entail.

3. Enhanced CDD

a. Scope

The 2017 Money Laundering Regulations (as amended in 2019) state:

> "33.—(1) A relevant person must apply enhanced customer due diligence measures and enhanced ongoing monitoring, in addition to the customer due diligence measures required under regulation 28 and, if applicable, regulation 29, to manage and mitigate the risks arising—
> (a) in any case identified as one where there is a high risk of money laundering or terrorist financing—
> (i) by the relevant person under regulation 18(1), or
> (ii) in information made available to the relevant person under regulations 17(9) and 47;
> (b) in any business relationship with a person established in a high-risk third country;
> (c) in relation to correspondent relationships with a credit institution or a financial institution (in accordance with regulation 34);
> (d) if a relevant person has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP (in accordance with regulation 35);
> (e) in any case where the relevant person discovers that a customer has provided false or stolen identification documentation or information and the relevant person proposes to continue to deal with that customer;(f) in any case where—
> (i) a transaction is complex or unusually large,
> (ii) there is an unusual pattern of transactions, or
> (iii) the transaction or transactions have no apparent economic or legal purpose, and
> (g) in any other case which by its nature can present a higher risk of money laundering or terrorist financing or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk third country."

b. Requirements

Legislation does not prescribe exactly what steps enhanced due diligence should entail. But it is clear within the scope of enhanced due diligence it is expected that more in-depth checks are undertaken, particularly source of funds and source of wealth to be understood and verified (especially where politically exposed persons (PEPs) are concerned). The Money Laundering Regulations 2019 (reg. 33) also state that in any case where:

> "(i) a transaction is complex and unusually large, or there is an unusual pattern of transactions, or
> (ii) the transaction or transactions have no apparent economic or legal purpose"

the enhanced CDD measures must include:

> "(a) as far as reasonably possible, examining the background and purpose of the transaction, and

(b) increasing the degree and nature of monitoring of the business relationship in which the transaction is made to determine whether that transaction or that relationship appear to be suspicious."

Additionally, the Money Laundering Regulations (reg. 33) state that depending on the requirements of the case, the enhanced customer due diligence measures may also include, among other things:

"(a) seeking additional independent, reliable sources to verify information provided or made available to the relevant person;
(b) taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;
(c) taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;
(d) increasing the monitoring of the business relationship, including greater scrutiny of transactions."

In regard to customers and transactions in high-risk third countries, the regulations state:

"The enhanced due diligence measures taken by a relevant person for the purpose of paragraph (1)(b) must include—
(a) obtaining additional information on the customer and on the customer's beneficial owner; (b) obtaining additional information on the intended nature of the business relationship;
(c) obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
(d) obtaining information on the reasons for the transactions;
(e) obtaining the approval of senior management for establishing or continuing the business relationship;
(f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination."

Where the customer—
(a) is the beneficiary of a life insurance policy, (b) is a legal person or a legal arrangement, and
(c) presents a high risk of money laundering or terrorist financing for any other reason,
An obliged entity that is a credit or financial institution must take reasonable measures to identify and verify the identity of the beneficial owners of that beneficiary before any payment is made under the policy.

The legislation does not envisage material differences between the requirements applicable to the various types of obliged entities. It depends mostly on whether there are identified high-risk factors such as geography and the presence of PEPs. As with other uses of the term "high risk", there may be a tension between professional judgment by insiders and more generic available

third-party assessments such as by the EC or by the not-for-profit Basel Institute or commercial bodies such as Bureau van Dijk, LexisNexis and Refinitiv (in alphabetical order). The analytical defensibility of such risk judgments is too large an issue for this paper, but it seems that the judgments of 'risk' mainly reflect the judgments of FATF and allied bodies, supplemented by public reported cases, rather than some underlying conceptual or sophisticated empirical approach. For example, though there are cases (prosecuted or not) that indicate the presence of money laundering in certain activities, and predicate crimes as occurring in particular countries more than others, the relationship between these and the confident 'risk ratings' is tenuous and would not normally meet the scientific standards of criminology. To the extent that the analyses conducted by the FATF, EU, UN and other bodies are conceptually and empirically weak, the evidence base for risk decisions will be likewise. There is no evidence that the work of civil society bodies such as Global Witness or investigative journalism is factored significantly in, nor is there any very serious analysis of the multi-jurisdictional nature of money trails and riskiness, which is still seen largely as a property of a country or a commodity rather than of a network of countries. This question of how cut-off points of riskiness are reached *and are empirically defensible* is an ongoing issue, as the EU list of high risk countries (un)surprisingly excludes EU (and one former EU) countries, despite strong evidence of high levels of money laundering there. The attribution of risks to *countries* rather than chains of relationships is too large an issue to be treated here.

c. Further Enhanced CDD Guidance

It is the same guidance as above listed. Guidance issued by the various supervisory bodies carries equal weight for the respective parts of the industry. One of the more comprehensive pieces of guidance is the one issued by the JMLSG[68]. However, the purpose of this guidance is to provide direction and examples of best practices. It is not binding, as it leaves scope for flexibility and interpretation of the exact implementation of the key principles. Furthermore, though the guidance can be referenced in a court, compliance with it does not give absolute immunity from prosecution. In terms of enhanced CDD, available guidance articulates the requirements in the Money Laundering Regulations 2017 (as amended in 2019) and also places a focus on understanding the source of wealth and funds of the client, the background to and purpose of the transaction. How a randomly selected jury in a criminal court or even a more expert regulatory tribunal is expected to or actually does make sense of these issues is a separate set of problems that would repay social scientifically informed policy analysis, which might vary between countries depending on their rules of evidence admissibility, jury selection et cetera.

[68] http://www.jmlsg.org.uk.

4. *Rules on Politically Exposed Persons*

a. Definition

The UK's Money Laundering Regulations define a PEP as:

> (a) "politically exposed person" or "PEP" means an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official;
> (b) "family member" of a politically exposed person includes—
> (i) a spouse or civil partner of the PEP;
> (ii) children of the PEP and the spouses or civil partners of the PEP's children;
> (iii) parents of the PEP;
> (c) "known close associate" of a PEP means—
> (i) an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with a PEP;
> (ii) an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP."

A reference to a business relationship with an individual includes a reference to a business relationship with a person of which the individual is a beneficial owner.

Individuals entrusted with prominent public functions include:

(a) heads of state, heads of government, ministers and deputy or assistant ministers;
(b) members of parliament or of similar legislative bodies;
(c) members of the governing bodies of political parties;
(d) members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
(e) members of courts of auditors or of the boards of central banks;
(f) ambassadors, charges d'affaires and high-ranking officers in the armed forces;
(g) members of the administrative, management or supervisory bodies of State-owned enterprises;
(h) directors, deputy directors and members of the board or equivalent function of an international organisation.

According to the Money Laundering Regulations, for the purpose of deciding whether a person is a known close associate of a PEP, a relevant person need only have regard to information which is in its possession, or to credible information which is publicly available. No epistemological guidance is given as to how organisations should judge whether or not information is "credible".

There are no differences in the *legal* definition. However, the FCA's guidance[69] does distinguish between domestic and foreign PEPs. The FCA advises that domestic PEPs can be treated as carrying a lower risk than foreign PEPs, perhaps reflecting its judgment or assumption that there is greater integrity among UK than foreign public officials: "A PEP who is entrusted with a prominent public function in the UK should be treated as low risk, unless a firm has assessed that other risk factors not linked to their position as a PEP mean they pose a higher risk." The FCA has allowed for such approach based on reg. 33 (6) of the Money Laundering Regulations 2017 (as amended in 2019), which states that when assessing whether there is a high risk of money laundering or terrorist financing in a particular situation, and the extent of the measures which should be taken to manage and mitigate that risk, obliged entities must take account of risk factors including, among other things, the country risk factors. According to the regulations, in making the assessment, obliged entities must bear in mind that the presence of one or more risk factors may not *always* indicate that there is a high risk of money laundering or terrorist financing in a particular situation.

The regulations state in what situations risk is typically considered high but also allow for a contextualised assessment of the risk, i.e. neither simplified nor enhanced due diligence have to apply automatically – a typical risk factor may be assessed not to pose a high risk in certain situations. Simplified CDD can only take place following risk assessment and if that assessment demonstrates the risk is low, then simplified measures can apply. That said, the actual risk assessment already entails some research, which arguably defeats the purpose of simplified CDD being applied, namely to reduce costs and ease business.

When interpreting the legal definition of a PEP, the FCA's guidance advises:

(a) it does not include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries;
(b) in the UK, it will not normally be necessary to treat public servants below Permanent or Deputy Permanent Secretary as having a prominent public function;
(c) firms should note that the Regulations (reg. 35(10)) explicitly state that they cannot apply these measures to those who were not a PEP under the Money Laundering Regulations 2007 (i.e. those who held a prominent public position in the UK (such as a former MP, retired member of the House of Lords or a former UK ambassador) where they ceased that office prior to 26 June 2017).

The FCA guidance allows for lower due diligence standards to be almost automatically applied in regards to local PEPs and excludes local government from the PEP definition even though

[69] Financial Conduct Authority, "FG 17/6 The treatment of politically exposed persons for anti-money laundering purposes", July 2017, https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf.

senior figures at local level (e.g. the Mayor of London) may have access to leverage and public funds equal to that at national level. This appears to contradict the spirit of the 4AMLD, which places scrutiny on both domestic and foreign PEPs and excludes middle and junior ranking officials but not necessarily those at a local level. Whether in the UK or in Canada, "Organised crime" penetration and corrupt contracting can also occur at a local level: it is a common assumption of policy-makers to focus on national-level criminality, without a proper appreciation of regional or local risks, perhaps because it is assumed that organised criminals want to play a national role, whether criminal or apparently legitimate after laundering their proceeds successfully. (This might be a consideration for British Columbia v Canada as a whole, just as it might be for, say, Glasgow or Manchester v. the UK as a whole.)

b. Requirements

PEPs must be the subject of enhanced due diligence. According to the UK's Money Laundering Regulations, the obliged entity must assess the risk that may arise from a relationship with a PEP/close associate or family member and on this basis determine what risk-management systems and procedures are appropriate.

The obliged entity is required to:

(a) have approval from senior management[70] for establishing or continuing the business relationship with that person;
(b) take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship or transactions with that person; and
(c) where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that person, including greater scrutiny of transactions.

The obliged entity will have to understand the background and purpose of the transaction and determine what level of monitoring would be appropriate.

Depending on the circumstances of the case, the enhanced due diligence measures may also include:

– seeking additional independent, reliable sources to verify information provided or made available to the obliged entity;
– taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;

[70] According to the regulations, "senior management" means an officer or employee of the relevant person with sufficient knowledge of the relevant person's money laundering and terrorist financing risk exposure, and of sufficient authority, to take decisions affecting its risk exposure.

– taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship.

The above measures do not always differ from those applied to other high risk factors, although legislation appears to place a focus on understanding the source of wealth and funds and obtaining approval from senior management when the client relationship involves a PEP risk factor.

5. *Rules on High-risk Third Countries*

a. Scope

A "high-risk third country" means a country which has been identified by the European Commission in delegated acts adopted under Article 9.2 4A MLD as a high-risk third country. This, like FATF black and grey listing, can be an issue of some political controversy though as noted earlier, its analytical defensibility is (or should be) also important.

The Money Laundering Regulations (reg. 33.6.c.) explain that enhanced CDD must be applied where risk posed by geographical risk factors is high, including:

> "(i) countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering or terrorist financing;
> (ii) countries identified by credible sources as having significant levels of corruption or other criminal activity, such as terrorism (within the meaning of section 1 of the Terrorism Act 2000(1)), money laundering, and the production and supply of illicit drugs;
> (iii) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
> (iv) countries providing funding or support for terrorism;
> (v) countries that have organisations operating within their territory which have been designated—
> (aa) by the government of the United Kingdom as proscribed organisations under Schedule 2 to the Terrorism Act 2000(2), or
> (bb) by other countries, international organisations or the European Union as terrorist organisations;
> (vi) countries identified by credible sources, such as evaluations, detailed assessment reports or published follow-up reports published by the Financial Action Task Force, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development or other international bodies or non-governmental organisations as not implementing requirements to counter money laundering and terrorist financing that are consistent with the

recommendations published by the Financial Action Task Force in February 2012 and updated in October 2016."

b. Requirements

The CDD rules for high-risk countries may be similar to the aforementioned enhanced CDD. For instance, the source of wealth and funds may need to be understood and verified in the case both of a PEP from a low-risk jurisdiction but who has attracted controversy in the media (e.g. for business activities or conspicuous expenditure) and of a client in wealth management who is not a PEP but comes from a high-risk jurisdiction. According to the Money Laundering Regulations, enhanced due diligence and enhanced monitoring must be undertaken to mitigate the risks arising in any business relationship with a person established in a high-risk third country or in relation to any relevant transaction where either of the parties to the transaction is established in a high-risk third country.[71]

The obliged entity will have to understand the background and purpose of the transaction and determine what level of monitoring would be appropriate.

Depending on the circumstances of the case, the enhanced due diligence measures may also include:

- seeking additional independent, reliable sources to verify information provided or made available to the obliged entity;
- taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction;
- taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;
- increasing the monitoring of the business relationship, including greater scrutiny of transactions.

The enhanced due diligence measures taken by an obliged entity for the purpose of a relationship or transaction with exposure to a high-risk third country must include—

(a) obtaining additional information on the customer and on the customer's beneficial owner; (b) obtaining additional information on the intended nature of the business relationship;

[71] It remains to be seen how the various industry associations, including the JMLSG, will interpret the 2019 amendments and guide the regulated sector. See https://jmlsg.org.uk/guidance/current-guidance/ for the latest guidance approved by HM Treasury in August 2020.

(c) obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;

(d) obtaining information on the reasons for the transactions;

(e) obtaining the approval of senior management for establishing or continuing the business relationship;

(f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

6. Private Sector CDD Guidance

Various vendors such as Bureau van Dijk, LexisNexis and Refinitiv – and numerous financial consulting firms - provide guidance. The Wolfsberg principles – developed by elite international banks - are also commonly referred to in the industry for legitimation of risk judgments. There are no material differences between the various pieces of guidance.

PRELIMINARY RISK ANALYSIS

Obliged entities are required to undertake money laundering and terrorist financing risk assessments both in terms of their enterprise generally (e.g. type of clients, product risk, geography) as well as of their clients and transactions specifically. Even when obliged entities plan to apply simplified CDD, they must first demonstrate that the risk is low by undertaking and documenting risk analysis.

More specifically, according to the Money Laundering Regulations, in carrying out the risk assessment, obliged entities must take into account information made available to them by the supervisory authority and risk factors including factors relating to:

(a) its customers;
(b) the countries or geographic areas in which it operates;
(c) its products or services;
(d) its transactions; and
(e) its delivery channels.

In deciding what steps are appropriate, obliged entities must take into account the size and nature of its business.

7. *First-time Reporting*

a. Trigger for/Degree of Suspicion

Under POCA, persons in the regulated sector (i.e. obliged entities) are required to make a report in respect of information that comes to them within the course of a business in the regulated sector:

- where they know; or
- where they suspect; or
- where they have reasonable grounds for knowing or suspecting.

that a person is engaged in, or attempting, money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as "grounds for knowledge or suspicion".[72]

The suspicion threshold is very low. As the JMLSG notes, suspicion is more subjective and falls short of proof based on firm evidence. Suspicion has been defined by the courts as being beyond mere speculation and based on some foundation: "[a] degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not"; and "[a[lthough the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation."[73]

Suspicion might be regarded more analytically as a matter of degree, not a binary construction. It is important to understand that this can be an organisational issue – as many as 150 people or as few as one might work under an MLRO, depending on the size of the regulated body. In *R v da Silva*,[74] the Court of Appeal considered the 'correct' interpretation of suspicion within the meaning of section 93A(1)(a) of the Criminal Justice Act 1988 (the predecessor to POCA). It was defined as:

> "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'."

[72] https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities. JMLSG Guidance, Part 1, chapter 6 "Suspicious activities, reporting and data protection", para 6.1, June 2020.
[73] JMLSG Guidance, Part 1, chapter 6 "Suspicious activities, reporting and data protection", para 6.11, June 2020.
[74] [2006] 2 Cr App R 35.

In its recent review, the Law Commission concluded that:

> "the large volume of disclosures was caused, in part, by a broad definition of "criminal property" in section 340 of POCA which requires that suspected laundering of the proceeds of any criminal conduct must be reported … Around 15% of authorised disclosure SARs did not meet the threshold of suspicion. If we assume that this proportion is representative across all 27,471 authorised disclosures submitted between October 2015 and March 2017, approximately 4,121 would have been submitted unnecessarily … [R]eporters only articulated reasonable grounds to suspect, by demonstrating one or more objective grounds, in 52.4% of the sample we analysed. This represents a substantial proportion of authorised disclosures which are lodged without objective grounds in support."[75]

Without a statutory definition or well developed guidance as to the meaning of suspicion:

(a) suspicion is a low threshold if it requires only a possibility which is more than fanciful. The application of this criterion will normally lead to a large number of reports, and many false positives and/or SARs that there are insufficient resources to investigate in a more than minimal way;

(b) without a clear definition, guidance or a requirement for reasonable grounds, suspicion can be inconsistently applied by those who have to decide whether or not to report their concerns.

The exception is where there is professional legal privilege, where there is an exception to the duty to report: an issue that will be examined separately.

b. Content and Direct Addressee(s) of SARs

The SAR is filed with the UK's FIU, which sits within the NCA. It is normally filed through the SAR online system, though there is a capacity to file manually, which is discouraged by the FIU since it involves them in more work. How the SAR is filed has no formal bearing on the way SARs are prioritised; it is an issue of administrative cost and convenience, as all bodies seek to promote the shift from manual to electronic communication to reduce the burden on their scarce resources.

According to guidance provided by the NCA,[76] the "Reason For Suspicion" field must set out the facts, focusing on who is involved, what and where the criminal/terrorist property is and its value

[75] Law Commission, "Money Laundering: Summary", 2019, p. 8, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2019/06/6.5612_LC_Anti-money-laundering-summary_v6.pdf.

[76] National Crime Agency, "Requesting a defence from the NCA under POCA and TACT", April 2018; updated version as of May 2019; https://www.nationalcrimeagency.gov.uk/who-we-are/publications/43-requesting-a-defence-under-poca-tact/file.

(estimated as necessary), when and how circumstances arose and are planned to happen, and ultimately why the reporter is suspicious or has knowledge.

Details on the entities involved (these entities may be the subject of the SAR themselves or may be linked to an individual who is the subject of a SAR; they may be the client or a client's counterparty if the SAR is actually not on the client but the client's counterparty) should include:

- subject's full name, date of birth and addresses (including postcode);
- subject details (e.g. National Insurance numbers, vehicle registration, driving licence, passport number, phone numbers, email addresses, etc.;
- subject's occupation/employer;
- details of any associated subjects (including, where appropriate, full details of professionals involved in the activities);
- company details, including full legal name, designation (Ltd, LLP, GmbH, SARL), registration number and tax reference/VAT numbers, country of incorporation and details on beneficial ownership where held);
- if relevant to the business, the subject's financial details (account numbers) and details of associates.

c. Duty not to Disclose

Under POCA, it is a criminal offence to release information to the customer that a SAR has been submitted. This is called a "tipping-off offence". The customer is very likely to suspect that a SAR has been made if the transactions they want to make are significantly delayed or frozen altogether. The banks have developed forms of words to give to customers without committing tipping-off offences. For instance, where banks need to obtain information from a client about a transaction that has been flagged up by automated systems as potentially suspicious, banks may simply refer to the need to update their KYC. Banks will avoid mentioning suspicion or anything that suggests the transaction is being investigated for money laundering or terrorist financing concerns. Some organisations use general wording such as "compliance with statutory obligations" when they have to explain a delay in a transaction; but in the industry there is a view that this wording will be commonly associated with obligations arising from AML/counter-terrorist financing legislation. What offenders or non-offenders think if and when they are given such explanations is germane to the effectiveness of these anti-tip-off provisions, but not to this report. It is less consequential in the UK, where reporting does not automatically lead to a freeze on the transaction or the account, than in some other jurisdictions.

d. Power or Duty to Freeze

In the UK there is a "defence", also known as "consent", regime. Persons and businesses generally, and not just those in the regulated sectors, may avail themselves of a defence against money laundering charges, referred to colloquially (and somewhat pejoratively, since the implication is that this not a real request for consent), as DAML or DATF (defence against terrorist financing). This can be done by seeking, via a SAR, the consent of the UK's FIU at the NCA. This consent is to conduct a transaction or undertake other activity about which they have concerns. For DAML the legislation gives the NCA seven working days to respond. Where no reply is provided by the NCA, it is considered that a defence is afforded to a reporter at the end of the seven-day notice period. Where the NCA refuses consent, the transaction or activity must not proceed for a further 31 calendar days, or, if earlier, until further notified by the NCA.[77] The moratorium period of 31 calendar days can be extended. When it comes to terrorist financing, however, where the consent request has been refused, there is no moratorium period, and there is no defence unless and until the request is granted by the NCA.

The regulated entity is expected to continue monitoring the activity in any event, regardless of whether a consent has been granted. The consent does not absolve the reporter from any of their other AML/counter-terrorist financing obligations.

8. Follow-up

a. Duty to Provide FIU with Additional Data

If the FIU requires further information, the reporting entity will be expected to provide it. In principle, the FIU can ask for any additional information and obliged entities will have to provide it, unless legal privilege applies.

b. Continued Duty not to Disclose SAR to Client

The regulated entity is expected not to disclose the filing of the SAR to the client under any circumstances. The fact that a SAR has been made is not disclosed in evidence to the defence in the event of a criminal trial, though it may be the subject of a civil suit against the disclosing body if a plaintiff/"victim" claims that it has been *improperly* harmed by freezing of funds, etc.

[77] This regime has been reviewed by the Law Commission (2018, 2019) and in late 2020 is awaiting a government decision as to what action should be taken.

c. Continued Collateral Duties

The obliged entity is expected to carry on fulfilling its general AML/counter-terrorist financing duties such as continuing to apply ongoing KYC, due diligence and monitoring measures unless the obliged entity has decided to offboard the client.

d. Limits to Request Information from Obliged Entities in Case of Suspicion

There are no limits as long as the request of information does not constitute tipping-off. However, guidance provided to the legal sector makes clear that responses to requests from law enforcement agencies must factor in legal professional privilege (LPP), which is not overridden by such requests.[78]

Regulated persons are prevented from disclosing if their knowledge or suspicion is based on privileged information and LPP is not negated by the crime/fraud exception (e.g. a law firm cannot use LPP to assist an offender to commit a crime that has not taken place). It is the Legal Sector Affinity Group's view[79] that the regulated person will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence. (The Legal Sector Affinity Group represents the shared view of all the regulatory bodies in the legal sector.)

9. *Special Rules for Privileged Professions*

a. Trigger for/Degree of Suspicion

There may be a defence where the information has been provided in privileged circumstances and/or is protected by LPP.

---

[78] Legal Sector Affinity Group, "Anti-Money Laundering Guidance for the Legal Sector", March 2018 (currently awaiting approval for 2020 revisions). For an important recent case on when LPP is entitled to be claimed and by whom, see *Serious Fraud Office v Eurasian Natural Resources* [2018] EWCA Civ 2006.

[79] This and other pieces of guidance (e.g. by the JMLSG) are arguably an interpretation of legislation and provide examples of best practices. In this sense, it is generally expected that the industry complies with the guidance. However, as it remains guidance, obliged entities may approach measures differently from those laid out in available guidance as long as they are able to demonstrate that they have applied an appropriate reasoning consistent with the aims of the legislation. Guidance is not meant to cover every eventuality and (despite what behavioural scientists might term pressures towards 'herding' behaviour) there may be circumstances in which an obliged entity has found an approach that arguably is more appropriate and better than what is said in the guidance, and puts that into practice.

Specifically, the above-mentioned Legal Sector Affinity Group's current guidance (under revision) notes:

> "When advice is given or received in circumstances where litigation is neither contemplated nor reasonably in prospect, except in very limited circumstances communications between you and third parties will not be protected under the advice arm of LPP.
>
> Privileged circumstances, however, exempt communications regarding information communicated by representatives of a client, where it is in connection with your giving legal advice to the client, or the client seeking legal advice from you."[80]

This guidance applies to the entire legal sector, i.e. tax advisors would be included if they provide tax advice in their capacity as independent legal professionals.

The guidance also explains:

> "No offence is committed if the information or other matter giving rise to suspicion comes to a professional legal adviser or relevant professional advisor in privileged circumstances.
>
> You should note that receipt of information in privileged circumstances is not the same as legal professional privilege. It is a creation of POCA designed to comply with the exemptions from reporting set out in the European directives.
>
> Privileged circumstances means information communicated:
>
> – by a client, or a representative of a client, in connection with the giving of legal advice to the client; or
> – by a client, or by a representative of a client, seeking legal advice from you; or
> – by a person in connection with legal proceedings or contemplated legal proceedings.
>
> The exemption will not apply if information is communicated or given to the legal professional with the intention of furthering a criminal purpose.
>
> The Crown Prosecution Service guidance for prosecutors indicates that if a legal professional forms a genuine, but mistaken, belief that the privileged circumstances exemption applies (for example, the client misleads the legal professional and uses the advice received for a criminal purpose) the legal professional will be able to rely on the reasonable excuse defence. …
>
> LPP does not extend to everything that legal professionals have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege.

[80] Legal Sector Affinity Group, "Anti-Money Laundering Guidance for the Legal Sector", March 2018 (currently under revision and approval by HM Treasury)

> The extent to which LPP attaches to a notary's records has not been the subject of a legal decision in England and Wales and is an evolving area of law. Notaries should therefore consider seeking specific legal advice based on the particular circumstances of a given situation if it appears LPP may apply. …
>
> LPP does not extend to documents which themselves form part of a criminal or fraudulent act, or communications which take place in order to obtain advice with the intention of carrying out an offence. …
>
> It is not just your client's intention which is relevant for the purpose of ascertaining whether information was communicated for the furtherance of a criminal purpose. It is also sufficient that a third party intends the legal professional/client communication to be made with that purpose. …
>
> If you know the transaction you're working on is a principal offence, you risk committing an offence yourself. In these circumstances, communications relating to such a transaction are not privileged and should be disclosed."[81]

As mentioned in previous sections, regulated persons are prevented from disclosing if their knowledge or suspicion is based on privileged information and LPP is not excluded by the crime/fraud exception. It is the Legal Sector Affinity Group's view that under those circumstances, solicitors will have a reasonable excuse for not making an authorised disclosure and will not commit a money laundering offence. This has not yet been tested in the courts.

b. Content and Addressee(s) of SARs

SARs are filed with the UK's FIU at the NCA, as for every category of regulated entity. LPP does not extend to everything that legal professionals have a duty to keep confidential. LPP protects only those confidential communications falling under either of the two heads of privilege – advice privilege or litigation privilege. The exemption will not apply if information is communicated or given to the legal professional with the intention of furthering a criminal purpose.

c. Duty not to Disclose to Client

As per the Legal Sector Affinity Group's guidance, a legal professional will not commit a tipping-off offence if the disclosure to a client is made for the purpose of dissuading the client from engaging in conduct amounting to an offence.

[81] Ibid.

It is a defence that a disclosure is made by a legal adviser to a client, or a client's representative, in connection with the giving of legal advice or to any person in connection with legal proceedings or contemplated legal proceedings.

Such a disclosure will not be exempt if it is made with the intention of furthering a criminal purpose.

The guidance from the Legal Sector Affinity Group further advises that enquiries of a client or a third party to help the firm decide whether the professional has a suspicion is not tipping-off unless they disclose that a SAR has been made or that a money laundering investigation is being carried out or contemplated. The offence of tipping-off only applies to the regulated sector.

10. Protection of a SAR's Source

The source is protected from the discovery process in which parties to litigation must reveal their documents to the other side.[82]

RECORD KEEPING

Obliged entities must retain:

- copies of, or references to, the evidence they obtained of a customer's identity, for five years after the end of the customer relationship; and
- details of customer transactions for five years from the date of the transaction.

In regard to suspicious activity reporting, obliged entities should also retain:

- details of actions taken in respect of internal and external reports of suspicions;[83] and
- details of information considered by the nominated officer in respect of an internal report where no external report is made.

Records of all internal and external reports should be retained for at least five years from the date the report was made.

---

[82] Eoin O'Shea, "Civil Liability Protection For Those Making Suspicious Activity Reports (SARs)", Reed Smith Client Alerts, 28 May 2015, https://www.reedsmith.com/en/perspectives/2015/05/civil-liability-protection-for-those-making-suspic?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

[83] "Internal" is in reference to any internal to the obliged entity escalations of potentially suspicious activity to the nominated officer who then decides whether a SAR needs to be filed "externally", i.e. with the FIU at the NCA.

COMPLIANCE OFFICERS

Regulated entities must nominate an officer to receive disclosures[84] from the regulated entity's staff under Part 3 (terrorist property) of the Terrorism Act 2000 or Part 7 (money laundering) of POCA.

According to the Money Laundering Regulations, where a disclosure is made to the nominated officer, that officer must consider it in the light of any relevant information which is available to the obliged entity and determine whether it gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion that a person is engaged in money laundering or terrorist financing.

It is the nominated officer's responsibility to decide whether they need to send a report or "disclosure" about the incident to the NCA (where the UK's FIU sits) by filing a SAR.[85]

Separately, for those obliged entities that are regulated by UK's financial services regulator (the FCA), the Handbook of the FCA, SYSC[86] 3.2.6I, stipulates that a firm must:

(a) appoint an individual as MLRO, with responsibility for oversight of its compliance with the FCA's rules on systems and controls against money laundering; and
(b) ensure that its MLRO has a level of authority and independence within the firm and access to resources and information sufficient to enable him to carry out that responsibility.

The FCA Handbook, SYSC 3.2.6J, further stipulates that the job of the MLRO within a firm is to act as the focal point for all activity within the firm relating to AML. The FCA expects that a firm's MLRO will be based in the UK.[87]

In FCA-regulated firms, the nominated officer and the MLRO can be the same person (see the JMLSG Guidance, 2017), and usually is; moreover, in non-FCA regulated firms the nominated officer can also be referred to as the MLRO.

Where the MLRO is sufficiently senior, that person can act also as the MLCP (see section III.A.1.c for details on MLCP above).

Depending on the size and nature of the business, the smallest organisations and sole practitioners do not have to have these three controls: (i) to appoint a MLCP, (ii) to screen

[84] In this context "disclosures" means escalations from internal staff of any suspicious financial activity that may entail money laundering or terrorist financing.
[85] https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities.
[86] The Senior Management Arrangements, Systems and Controls sourcebook (SYSC) is located within the high-level standards block of the FCA Handbook.
[87] https://www.handbook.fca.org.uk/handbook/SYSC/3/2.html#DES92.

employees, and (iii) to have an internal audit function. But all regulated persons are still required to comply with AML/counter-terrorist financing legislation and file SARs. Sole practitioners will have to perform the MLRO role.

The MLRO has to have independence and powers within the regulated entity, in order to be able to take decisions as appropriate, and also has to have the technical competence (e.g. for those entities regulated by the FCA, MLROs have to be approved by the FCA and so the FCA has to determine if the individual is sufficiently competent, as well as having a clean criminal and civil debt record). Typically, bigger organisations apply a three lines of defence model where the teams generating revenue and facing customers and their support functions (e.g. middle office and back office within banks) are within the first line of defence (KYC is often within first line of defence); the second line of defence is compliance and financial crime risk management oversight (including overseeing the KYC process occurring in the first line of defence); and the third line of defence is audit and controls assurance. The nominated officers and MLROs sit within the second line of defence and thus are independent, to the extent possible, from business while exercising oversight over the first line of defence."[88]

More broadly, Under the MLRs, HM Treasury is responsible for appointing AML/CTF supervisors. "Working closely with both statutory supervisors (FCA, HMRC and the Gambling Commission) and the 22 legal and accountancy PBSs, as well as with OPBAS, the Treasury seeks to ensure they deliver upon the government's objective of a robust and risk-based approach to supervision, applying dissuasive sanctioning powers when appropriate, while minimising unnecessary burdens on regulated firms. "[89] During 2018-19, the designated AML/CTF supervisors from professional bodies carried out 6,201 Desk-Based Reviews (DBRs) and visits in total, on a population of approximately 85,437. In a supervised population where 15% are classified as high risk, according to supervisors' returns, the overall proportion of the population who received a DBR or visit was 7.3%. In the same year, the FCA conducted 47 DBRs and 64 onsite visits (out of 19,660 firms): none of those in DBRs was assessed as non-compliant, but 14 were following onsite visits.

Frequent breaches identified in firms supervised by the FCA through their supervisory programmes include (para 3.21): inadequate client risk assessments; ineffective application of

[88] See https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/; Institute of Internal Auditors, "The Three Lines of Defense in Effective Risk Management and Control", IIA Position Paper, January 2013, https://global.theiia.org/standards-guidance/recommended-guidance/Pages/The-Three-Lines-of-Defense-in-Effective-Risk-Management-and-Control.aspx; Inês Sofia de Oliveira, David Artingstall and Florence Keen, with Matt Russell and Ben Luddington, "The Cartography of Compliance On Banks, Anti-Money Laundering and Achieving Effectiveness in the UK", Royal United Services Institute for Defence and Security Studies in cooperation with PWC, January 2017.

[89] *Anti-money laundering and counter-terrorist financing: Supervision report 2018-19*, HM Treasury, 2020, para 1.1.

enhanced due diligence, leading to poor identification and monitoring of high risk customers; inadequate AML policy procedures; and the lack, or inadequacy, of AML training for relevant staff. During the relevant period, the FCA took formal action on approximately 57% of the firms reviewed and approximately 52% of the firms visited. The distribution of these penalties is unavailable, but formal action can include appointing a 'skilled person' (at the expense of the business) or enforcement action such as financial penalties.

INTERNAL COMPLAINT MECHANISMS

The law does not require that there is a specifically designed "whistleblower" mechanism as such. But, reflecting contemporary views about the importance of openness, regulators require that all regulated entities put in place a process that informs senior management of both issues (e.g. violations, weaknesses in the internal systems and controls) and of relationships (e.g. with clients, business partners) that may represent a particularly high risk outside the organisation's acceptable risk parameters/risk appetite. Such mechanisms can be used both by internal and third-party employees. Separately, if employees of third persons know or suspect money laundering or terrorist financing (or, if they are within the regulated sector, have reasonable grounds to know or suspect) within an obliged entity, they should make a disclosure to the NCA.

FCA-regulated entities are required to appoint an MLRO (subject to FCA approval), who is expected to prepare an annual MLRO report for senior management to inform them of any material issues and AML/counter-terrorist financing developments within the organisation.[90]

Separately, it is also expected from each regulated entity (not just those regulated by the FCA) to have a whistleblowing line. The FCA's Financial Crime Handbook lists as an example of good practice: "Whistleblowing procedures are clear and accessible, and respect staff confidentiality."[91] For firms' obligations in relation to whistle-blowers, the FCA Handbook makes reference to the Public Interest Disclosure Act 1998.[92] Barclays Bank's CEO was fined £642,430 and reprimanded in 2018 for actively seeking (though unsuccessfully) to discover the

[90] http://www.jmlsg.org.uk/other-helpful-material/article/mlro-annual-report.

[91] Financial Conduct Authority, *Financial crime: a guide for firms,* Part 1: A firm's guide to preventing financial crime, July 2016. The FCA has announced a pending upgrading of its approach to whistleblowing: see "UK financial regulator to overhaul its treatment of whistleblowers", Financial Times, 30 December 2018. https://www.ft.com/content/3ebb9920-f4ae-11e8-ae55-df4bf40f9d0d. See, more generally, the website of Protect (https://www.pcaw.co.uk/), with whom the FCA is collaborating in these revisions. These are not linked specifically to AML: see, e.g. Financial Conduct Authority, "Retail and Wholesale Banking: review of firms' whistleblowing arrangements", 14 November 2018, https://www.fca.org.uk/publications/multi-firm-reviews/retail-and-wholesale-banking-review-firms-whistleblowing-arrangements.

[92] www.legislation.gov.uk/ukpga/1998/23/contents.

identity of an internal whistle-blower, though readers should note that this was not in the context of money laundering revelations, which might have been treated more punitively..[93]

Additional Preventive Measures

Documenting the CDD and risk assessment process and record keeping is mandatory. UK legislation does not set out in detail how requirements must be met. However, regulatory guidance indicates what is expected to be seen as best practice; for instance, what due diligence on trade finance transactions should entail, or how guarantors (as opposed to client borrowers or issuers) should be treated. MLROs are expected to record their reasons for not referring internally reported cases onwards to the FIU as SARs. Proper recording of what has been done to assess risk and actual due diligence are reviewed as part of the supervisory process and can lead to fines if considered inadequate: these are often a matter of disputable judgment.

In addition to the various levels of due diligence and risk assessment of clients, business partners and counterparties, regulated entities are required to undertake enterprise-wide risk assessment, monitoring of transactions and provide training to staff, and there is guidance as to the respective processes/steps these processes should entail. This applies to all obliged entities.

It is a standard practice for potential employees to be vetted by employers (to verify their CV and check for criminal backgrounds), though MLROs have additionally to be vetted formally by the FCA. In addition, as discussed above, regulated entities are expected to have 'effective' whistleblowing lines, though how effectiveness is judged would repay further consideration.

The FIU publishes annual reports in which it provides statistics and feedback on the SAR regime. It also provides typologies material and general feedback on SARs through seminars aimed at improving their quality (at least from their institutional perspective). An organisation can also arrange a visit from the UK's FIU for feedback on the SARs submitted by the organisation. Indeed, the Money Laundering Regulations state that "the NCA must make arrangements to provide appropriate feedback on the suspicious activity disclosures it has received at least once a year." However, it is not clear whether this provision was intended to require the NCA to provide feedback to individual obliged entities or, cumulatively, to the entire regulated sector. Furthermore, the same provision of the Regulations states that the feedback may be provided in any form the NCA thinks fit. In practical terms, this will be general feedback, for example how to get better in terms of level of detail, structure, clarity – as serves the purposes of the FIU within

[93] Financial Conduct Authority, "Final Notice: Mr James Edward Staley", Ref. JXS02208, 11 May 2018, https://www.fca.org.uk/publication/final-notices/mr-james-edward-staley-2018.pdf. As with many fines, the issue of proportionality in relation to income or profits may be queried, and though it avoided a long civil trial, many news, business and political sources regarded the sanction is being overly lenient, not banning him from the sector.

its own staffing and systems constraints – rather than on outcome of the SAR or concrete information on the direction of any formal investigation (although the direction may become clear if there is a freezing order, trial, etc., though these are statistically rare events). The UK's FIU also organises general feedback sessions with regulated bodies, such as the Law Society Money Laundering Task Force, though these too might not discuss specific SARs. There can be tensions with professional bodies, insofar as the FIU may resist improvements that require it to do more with the capacity it does not have. The term 'appropriate' remains undefined and to that extent, deficient in meaning.

RULES ON OBLIGED ENTITIES' CIVIL LIABILITY TOWARDS CLIENT

If a client suffers economic damage from CDD measures (e.g. by the sudden disruption of banking services) or the freezing of assets after the filing of an unjustified SAR, an obliged entity cannot be held responsible and forced to compensate the client if the SAR is filed in good faith. A 2012 court case – *Shah v HSBC* – supports this,[94] though see *Lonsdale v National Westminster Bank*[95] for a rare exception. Some banks whose SARs were leaked in the 2020 'FinCEN leaks' episode are concerned about potential civil suits from their clients and former clients: whether any of those will occur in the UK or involve UK clients of international banks is unknown at this early stage.

SUPERVISORY AUTHORITIES' ROLE

11. Supervisory Measures to Ensure Application of CDD and Other AML-related Obligations

UK Supervisors exercise oversight by undertaking routine checks as well as probes triggered by specific events (e.g. information provided by a whistleblower). They also undertake periodic thematic reviews, which include the treatment of foreign PEPs and e-money risks, which aim to guide practice and may lead to fines or other sanctions for control weaknesses if not adhered to.[96]

---

[94] [2012] EWHC 1283 (QB); see also Law Society, "Shah v HSBC – an update". 17 May 2012, http://www.lawsociety.org.uk/support-services/advice/articles/case-summaries/shah-v-hsbc-update/.

[95] [2018] EWHC 1843 (QB).

[96] Examples include: Financial Conduct Authority, "TR13/9 Anti-Money Laundering and Anti-Bribery and Corruption Systems and Controls: Asset Management and Platform Firms", October 2013, https://www.fca.org.uk/publication/thematic-reviews/tr13-09.pdf; "TR 13/3 Banks' control of financial crime risks in trade finance", July 2013, https://www.fca.org.uk/publication/thematic-reviews/tr-13-03.pdf; "TR18/3 Money Laundering and Terrorist Financing Risks in the E-Money Sector", 3 October 2018, https://www.fca.org.uk/publications/thematic-reviews/tr18-3-money-laundering-and-terrorist-financing-risks-e-money-sector; and "TR14/16 How small banks manage money laundering and sanctions risk: update", 14 November 2014,

For law enforcement authorities, collecting SARs and following up on SARs is a key preventive power allowing them to gather intelligence ahead of potential money laundering transactions. However in practice, for this preventative role to be applied requires speedier action than is practicable in all but a small number of cases, usually where a DAML request is put in and/or there is an instruction/request to prioritise a SAR.

12. Complaint Mechanism

Under the Public Interest Disclosure Act 1998, a worker who reports wrongdoing in the public interest is protected by law – this person cannot lose their job or be treated unfairly for blowing the whistle.[97]

As the UK government's website explains, the practical effect of this legislation (though this is merely advice, not set out in the legislation) is that:

> "You can tell your employer or a prescribed person anonymously but they may not be able to take the claim further if you haven't provided all the information they need.
>
> You can give your name but request confidentiality – the person or body you tell should make every effort to protect your identity.
>
> If you report your concern to the media, in most cases you'll lose your whistleblowing law rights."[98]

There is not one single authority to receive complaints. There are various prescribed persons or bodies, each dealing with a different issue. For instance, Chapter 10 of the Law Society Code of Conduct states that solicitors must report serious misconduct by any person or firm authorised by the Solicitors Regulation Authority (SRA), or any employee, manager or owner of such a firm to the SRA. This includes conduct relating to a criminal offence such as money laundering, and conduct in relation to breaches of the Money Laundering Regulations.[99] Whistle-blowers can

https://www.fca.org.uk/publications/thematic-reviews/tr14-16-%E2%80%93-how-small-banks-manage-money-laundering-and-sanctions-risk.

[97] https://www.gov.uk/whistleblowing; see also https://www.pcaw.org.uk/a-guide-to-pida/.

[98] https://www.gov.uk/whistleblowing/who-to-tell-what-to-expect.

[99] https://www.gov.uk/whistleblowing/who-to-tell-what-to-expect; http://www.sra.org.uk/solicitors/enforcement/solicitor-report/whistleblowing-to-the-sra.page.

report direct to the FCA allegations about regulated firms in the financial sector such as banks and e-money firms.[100]

Where the complaint is not a matter of whistleblowing but is known to the organisation that is the subject of the complaint, it can then be referred to an ombudsman, such as the Financial Services Ombudsman.[101]

STATISTICS ON SARs BY OBLIGED ENTITIES

From a few informal tip-offs from bankers to police in 1986 (author observations), the number of "suspicious transaction reports" by bankers and professionals to the UK NCIS (later replaced by SOCA and then the NCA) rose from a few hundred in 1991 to 15,114 in 1999 to 94,708 in 2003 – almost doubling after 9/11 – to 195,000 in 2005 (9, 600 of them from lawyers) to 463,938 in 2017–18 and 478,437 in 2018-19. Covid-19 excepted, there is no reason to expect the numbers to fall.

The UK's FIU's annual reports provide statistics on the SAR regime, including the number of SARs filed per sector. While a breakdown of amounts per sector is not provided, and neither is the outcome of such reports (which is only partially known by the FIU or by anyone else), the FIU provides the amount of assets seized (but not per sector) which are considered to be the result of actions following up SARs. In addition, the FIU provides case studies with case-specific (but redacted) details, including amounts and the nature of the predicate offence. Given the number of SARs in the UK (and some other current EU Member States, such as the Netherlands), follow-ups that might be realistic in a low-reporting jurisdiction would be very ambitious in the UK. However, the lack of feedback reduces the lesson-learning potential of the dataset.

The number of SARs and the sectors from which they emanate are set out below. The sums involved in individual SARs or SARs collectively are unavailable for any sector: indeed despite the urgings of FATF evaluators, it is not clear what the point of collecting amounts of so many SARs would be, and there would be massive resistance to doing so, given the strains on the FIU and the opportunity cost of generating the data.

Table 1. SARs submitted by all sectors, April 2018–March 2019

April 2018 to March 2019	Volumes	% of total	% comparison to 2017-18
Credit institution – banks	383,733	80.21%	3.29%

[100] For instance, according to the media, a whistle-blower reported to the FCA allegations that e-money firm Revolut failed to adequately respond to internal compliance concerns. See BBC report, 2 April 2019 https://www.bbc.co.uk/news/technology-47751945. (Accessed 27 September 2019.) The FCA took no formal action, after investigation.

[101] https://www.citizensadvice.org.uk/consumer/get-more-help/how-to-use-an-ombudsman-in-england/.

Credit institution – building societies	21,714	4.54%	10.56%
Credit institution – others	10,203	2.13%	-25.41%
Financial institution – MSBs	18,940	3.96%	-10.65%
Financial institution – others	24,911	5.21%	16.16%
Accountants and tax advisers	5,055	1.06%	-1.65%
Independent legal professionals	2,774	0.58%	4.29%
Trust or company service providers	23	0.00%	-56.60%
Estate agents	635	0.13%	-10.56%
High value dealers	481	0.10%	93.17%
Gaming (including casinos)/leisure (including some not under Money Laundering	4,163	0.87%	93.27%
Not under MLRs	5,805	1.21%	5.78%
Total	**478,437**	**100%**	**3.13%**

Source: National Crime Agency, "Suspicious Activity Reports (SARS) Annual Report 2019"[102]

Further fine-grained details of reporting are available in the SAR annual reports.[103]

IV. THE SYSTEM OF FINANCIAL INTELLIGENCE UNITS: INSTITUTIONAL AND FUNCTIONAL CHARACTERISTICS

1. Purpose and Tasks

The UK's FIU receives, analyses and distributes financial intelligence gathered from SARs, both actively and via its management of its database ELMER, which authorised financial investigators can consult. Though its role has remained substantially unchanged since its creation and its absorption into the NCIS in 1992, it has no separate constitutional status from the NCA, and its legal authority for this work derives from subsection (c) of section 1(5) of the Crime and the Courts Act 2013, which states:

> "The NCA is to have the function (the 'criminal intelligence function') of gathering, storing, processing, analysing, and disseminating information that is relevant to any of the following—(a) activities to combat organised crime or serious crime; (b) activities to combat any other kind of crime; (c) exploitation proceeds investigations (within the meaning of section 341(5) of the Proceeds of Crime Act 2002), exploitation proceeds orders … and applications for such orders."

[102] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019.
[103] The NCA publishes reports annually.

The number and proportion of SARs received that are actually analysed in detail and further intelligence developed before distribution is unknown, but the lack of development by the FIU was one of the issues criticised by FATF in its 2007 and 2018 evaluations. Common sense would suggest that with a volume of SARs as great as that of the UK's FIU, there would have to be huge centralised staffing in order to develop a "large" proportion of them. In a comparative context, one way of expressing this might be as a ratio of reports received to staff available. Thus, disregarding the post-FATF MER significant increase in personnel, in 2017-18, 84 staff had to deal with 463,938 SARs, which equals 5,523 SARs per staff member per year or – excluding abstractions, sickness and supervisory responsibilities – around 220 per staff member per working day. Each "SAR development" therefore has a significant opportunity cost in not processing other SARs. However, neither in the UK nor elsewhere have FATF mutual evaluation reports approached this level of sophistication in analysing resource allocation issues and trade-offs hitherto. It is obvious from these data that even if staffing doubled, the number of SARs is far too great to permit serious intra-FIU investigation, even with improved technology such as that aimed for in the forthcoming SARs reform programme, partly to be financed by an Economic Crime Levy on regulated persons.

2. Independence

The UK's FIU is an operationally independent part of the NCA. In accordance with the strategic framework which set up the NCA, the Home Secretary determines the strategic priorities of the NCA and will hold the Director General of the NCA to account for the discharge of the "NCA functions" while also respecting the Director General's operational independence. More specifically, in regard to operational independence, the framework explains that NCA's Director General is:

> "responsible (including through a senior NCA officer acting on his or her behalf) for all decisions about which operations to conduct and how they should be conducted. This would include, for example, decisions about whether to continue or stop a criminal investigation."[104]

Nor can prosecutors or other police forces/non-police agencies such as HMRC instruct it to carry out further investigations without the agreement of the NCA Director General, though they can request further enquiries. By convention, the Director General does not give instructions to the FIU on what to follow up or not follow up, and there is no evidence of political interference in the FIU work, though such interference would be public only in the event of whistleblowing.

[104] Crime and the Courts Act 2013, sections 3 and 4. See also Home Office and NCA, "Revised Framework document for the National Crime Agency", May 2014, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/29-nca-framework-document/file.

However, as with many aspects of the unwritten UK constitutional arrangements, this independence operates by convention.

3. Powers

The UK's FIU has analytical but no coercive powers, except limited ones over DAML freezing orders that are carried out by a separate NCA team. In the vast majority of cases, no legal consequences flow from the making of a SAR, and no action is taken automatically against an individual or business that is reported on. It is not known how many subjects of SARs are subsequently de-risked by their bank without being told that they have been reported to the FIU (which would be a criminal tipping-off offence). However, de-risking following SARs is by no means automatic, and we should not underestimate the impact of the cost of enhanced scrutiny impacted by more general risk profiling by regulators and international risk matrices on discouraging risk-averse banks from "risky" clients.

The JMLSG explains that POCA empowers the NCA to conduct an investigation to discover whether a person holds criminal assets and to recover the assets in question.

POCA also creates five investigative powers for the law enforcement agencies, which are therefore available to the NCA and to other agencies (but not to the UK's FIU uniquely): a production order; a search and seizure warrant; a disclosure order; a customer information order; and an account monitoring order.

TREATMENT OF SARS

4. Data Processing

No SAR leads to the automatic blocking of funds in the UK. SARs are increasingly but not exclusively electronic, and since the beginning of the SAR regime, there have never been sufficient resources to do more than analyse a minority of them. The FIU operates an electronic database called ELMER on which SAR data are kept for six years, following intervention by the Information Commissioner to reduce the period for which they were kept.[105] The FIU makes a judgement about which police force to forward the SAR to, but with the exception of the Serious Fraud Office (SFO), the UK does not operate a prosecutor-led system of investigation, and

[105] For a thorough Parliamentary report on the data retention and processing issues at the NCA's predecessor agency, SOCA, see https://publications.parliament.uk/pa/ld201011/ldselect/ldeucom/82/8205.htm.

prosecutors do not get access to SARs. The UK's FIU operates a "consent regime",[106] under which SAR reporters can request permission to transact funds transfers (when a suspicion has emerged prior to a transaction), giving them a defence against money laundering or terrorism financing charges.[107] Relevant statistics on consent requests is provided in the table below.

Table 2. Statistics on consent requests, 2018-2019

Key statistics	April 2018 to March 2019
Total SARs	478,437
DAML SARs	34,151
DAML SARs refused	1,332
Breaches of confidentiality	3

Source: National Crime Agency.

"The NCA is not a crime reporting agency. If the funds involved are not yet the proceeds of crime then it is not money laundering, but attempted fraud."[108] This statement is clearly aimed at reducing defensive (or precautionary; not to be confused with 'defence/consent' requests) filing but fails to recognise various subtleties. For instance, in all countries in which it is a predicate crime for laundering, fraud is typically also laundering at the same time (e.g. tax fraud, investment fraud) and on this basis, attempted fraud is also attempted money laundering. There may be scenarios where the offence is in the process of being committed and so the funds are already tainted, and because of the broad legal definition of money laundering it is difficult for obliged entities to draw a line. For instance, if a bank sees payments from a client to a counterparty suspected to be a public official, with the payments suspected to be bribes for the official to organise a fraudulent bidding process, then the client has not generated proceeds yet, but the funds the client is sending to the official are crime proceeds for the official. Making that corrupt payment, even if the client has not won the bid yet and has not generated corrupt proceeds, is already an offence. Although the NCA probably did not mean to discourage the reporting of such conduct, the NCA's above statement may be interpreted in that manner. It is

[106] Some in the industry view it as controversial because consent should not be seen as " clearance " from the NCA and does not absolve obliged entities from responsibility (other than from the ML offences under POCA) if they believe the funds are criminal; for instance, consent is not a defence under the UK Bribery Act. This appears to defeat the purpose of obtaining consent. Additionally, with the transaction delayed , the client will likely draw the conclusion that a SAR has been made and will in practice be unintentionally tipped off (communication must be carefully worded to avoid the "tipping-off" offence). With no *de minimis* thresholds and with loosely defined concepts, the SAR regime has been criticised by the Law Commission for the high volume of low-quality defensive (or precautionary) SARs.

[107] For the NCA's interpretation of the issues, see National Crime Agency, "Requesting a defence from the NCA under POCA and TACT", May 2019.

[108] See National Crime Agency, "Guidance on submitting better quality Suspicious Activity Reports (SARs)", 2019, p. 5, https://www.nationalcrimeagency.gov.uk/who-we-are/publications/42-guidance-on-submitting-better-quality-sars/file.

also worth noting that POCA (section VII, 330) requires not only the reporting of persons involved in laundering and the whereabouts of laundered property, but also any information which an individual believes or it is reasonable to expect him to believe may assist in identifying these persons or the whereabouts of any of the laundered property. What information may assist is a subjective decision; and so obliged entities who are risk-averse find themselves having to report even a very remote nexus that in reality may be of no help to the NCA. This process of working out and mitigating the unintended consequences of legal rules is important not just for the UK but also for Canada and any country.

The UK's FIU receives financial intelligence gathered from SARs, and makes all SARs available to approximately 4,800 authorised financial investigators in law enforcement agencies and to HMRC for their own analysis and investigations (with the exception of SARs in certain sensitive categories such as professional standards investigations).[109]

5. *Special Procedures for Privileged Professions*

There are no specific differences between how a SAR from a non-privileged obliged entity and how a SAR from a privileged profession would be processed. However, LPP can be a reason for not reporting and for having a defence against a charge of money laundering, except when used to further a crime. But if the FIU is seeking to develop a SAR, it and criminal investigators cannot lawfully read or use material that is under LPP if they come across it, and will be denied access to it if they ask for it. Such claims of LPP are normally given to a separate set of senior lawyers who have no contact with an investigation, to assess whether or not the material is legally privileged.

6. *Feedback Obligations*

a. Obligation of the FIU

The obliged entity will seldom be aware of what has happened to a SAR, neither the court outcome (except where the case is reported in the media and the reporting body is aware of that) nor even the investigative input. This has been the case since the beginning of the system.[110] Except in special circumstances, such as the JMLIT, there is no legal authority for intelligence to

[109] See HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing 2017*, October 2017.
[110] Michael Gold and Michael Levi, *Money-Laundering in the UK: an Appraisal of Suspicion-Based Reporting,* London: Police Foundation, 1994.

be passed from the FIU or police organisation to the reporting entity. Consequently, feedback would be bound to be limited.

However, as discussed earlier, there is a consent/defence regime, in accordance with which, if the FIU wants a transaction that is subject to a SAR to be blocked, it must notify the obliged entity that had filed the SAR.[111]

Obligation of Investigative Authorities

The various agencies collaborate to the extent that they have the resources and good institutional and personal relationships to do so. However, the authority receiving the information is not under a formal obligation to provide feedback to the FIU and only sometimes does so. Generally, where a SAR has resulted in the seizure of assets, information is fed back to the FIU and then is reflected in the FIU's annual report as part of its statistics. However, since asset freezing and confiscation are decisions that are by no means all centralised in CPS, HM Courts and Tribunals Service and individual courts, these data are not guaranteed to be complete. HMRC is bound by its own data protection and secrecy rules, and does not feed back information to the FIU.

7. Disclosure Obligations towards "Suspect"

The FIU does not inform the "suspect" about a SAR. The suspect's defence cannot know about SARs officially, even if the suspects can work out by the non-availability of financial services that they have been the subject of a SAR and perhaps a DAML report.

PROACTIVE INVESTIGATIONS

The UK's FIU has no separate constitutional and legal powers. The FIU are on the staff of the NCA and in principle could conduct investigations without receiving SARs. However, in practice

[111] In *Lonsdale v National Westminster Bank* [2018] EWHC 1843 (QB), the High Court ruled that in some rare circumstances, a customer could challenge the basis for the making of a SAR. In March 2017 the bank froze a joint account belonging to one of its customers, a barrister, for eight days and in December it froze seven other accounts of the same customer. The customer requested access to documents relating to the freezing of his accounts. The bank provided limited documentary evidence and did not disclose the SARs. The judge emphasised that the general rule is that if a document is mentioned in a statement of case or a witness statement, the other party has a right to inspect it. However, a balance must be struck when considering whether, for example, inspection would be disproportionate or should be refused on grounds of confidentiality. The banks have learned to live with this uncertainty.
The judge held that there was no evidence that inspection by the plaintiff would amount to tipping-off, nor that the SARs, submitted some 16 months previously, were required still to be kept confidential, since there was no evidence of active investigation. The SARs were plainly relevant to the assessment of whether NatWest genuinely held a relevant suspicion, the key issue in Mr Lonsdale's claim for breach of contract. On that basis the judge ordered that the SARs be disclosed to Mr Lonsdale unless the NCA sought to argue otherwise within 14 days, which it did not.

they do not do so, and in any event they would not be doing so as members of the FIU but as NCA staff.

ACCESS TO DATA

The FIU does not have access to the intelligence data banks of other bodies. It can check the Police National Computer (PNC) for convictions and other data that are on the PNC, but not the tax, welfare payments, trading standards or databases of other public bodies. Those bodies can use the SARs for their own purposes and can collaborate with the NCA/FIU. It can also make requests to access foreign FIU and other data, via the Egmont Group or (via the UK Central Authority) using mutual legal assistance processes. As per the above, the FIU provides data to other parts of the NCA and other agencies. HMRC has direct access to the FIU's data. The FIU does not have access to other agencies' confidential data banks. It (and other law enforcement bodies) can request access to HMRC's register of trusts with UK tax consequences.

The FIU does not have automatic access to confidential private data banks but can request further information following up on a SAR. It purchases access to some commercial databases, as the private sector FIUs created within large banks (sometimes as big as the UK FIU) can also do.

8. Data Analytics

It is not clear that the FIU or any enforcement body would be prohibited from using data mining. However, there is no evidence that they actually are doing or will do so, beyond counter-terrorism. The FIU does data matching on its own database consisting of SARs, and it explores possible connectivity via JMLIT cases.[112]

The UK's FIU reports[113] the following activities that it undertakes (though the denotation of this work and of the category of 'vulnerable persons' remains vague):

> "The UKFIU screens/analyses SARs daily to identify fast-tracking to LEAs; this is to

[112] According to the NCA's website: "JMLIT is a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats. The taskforce consists of: over 40 financial institutions; the Financial Conduct Authority; Cifas; five law-enforcement agencies: the NCA, HMRC, the SFO, the City of London Police, and the Metropolitan Police Service. JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015, and is considered internationally to be an example of best practice." See https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre. Data fusion is, however, a complex legal and practical process.

[113] SARs Annual Report 2019, p. 7. (Below, "Read and triaged" refers to the total number of SARs returned by the UK's FIU keyword searching that require reading and triaging by a UK FIU officer; integrity SARs relate to knowledge or suspicion of money laundering and/or terrorist financing involving an employee of an LEA or the civil service.) See https://www.nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019.

ensure that the intelligence's maximum value is exploited. Over the year the UKFIU:

- 'read and triaged' 27,586 potential vulnerable person SARs (up 5.84%).
- disseminated 3,735 vulnerable person SARs (up 3.32%).
- read and triaged 25,800 potential politically exposed person (PEP) SARs (down 3.25%).
- disseminated 2,388 PEP SARs (up 68.29%).
- read and triaged 29,848 integrity SARs (down 4.51%).
- disseminated 788 integrity SARs (down 35.78%)."

The above are not substantially different forms of reporting but different statistical categories applied by the FIU.

9. International Cooperation

The FIU cooperates with counterparts abroad based on Memoranda of Association. The content of any such agreements is, however, confidential. There is a special agreement with the Crown Dependencies and Overseas Territories for access to beneficial ownership information and other financial intelligence, which has expanded in scope over time.[114] The NCA maintains a substantial number of international liaison officers internationally who can both make and respond to lawful requests.

PARTICIPATION OF "SUSPECTS"

10. Defence Rights

In theory, suspects should not be aware of a SAR being filed on them and an obliged entity should not be committing a "tipping-off" offence. Therefore, defence rights do not apply, especially in the context where assets are not frozen.[115]

---

[114] *Statutory review of the implementation of the exchange of notes on beneficial ownership between the United Kingdom, Crown Dependencies and Overseas Territories*, 2019.

[115] The pre-charge restraint order under POCA is a tool that can only be used in rare circumstances and is *not* a power of the FIU but only of the prosecutor. *In re Stanford International Bank Ltd v Serious Fraud Office* [2010] EWCA Civ 137, Hughes LJ said (para 191): "In effect a prosecutor seeking an ex parte order must put on his defence hat and ask himself what, if he were representing the defendant or a third party with a relevant interest, he would be saying to the judge, and, having answered that question, that is what he must tell the judge. … This application came close to being treated as routine and to taking the court for granted. It may well not be the only example."

If a SAR is used as part of an investigation that results in a trial, the suspect will have the same defence rights as any other defendant. However, typically during trial the fact that a SAR had led to the trial is not disclosed, nor is the name of the obliged entity. In very rare cases, there can be civil litigation in which the plaintiff has discovered the existence of a SAR or has plausibly surmised that one had been made and seeks damages against the reporting entity. As the *Shah v HSBC* case[116] indicates, where an obliged entity has filed a SAR in good faith, the court is expected to decide in favour of the obliged entity. In *Lonsdale v National Westminster Bank*,[117] the High Court ruled that in some rare circumstances a customer could challenge the basis for the making of a SAR, but only after a period of time has elapsed that makes it clear there is no longer any plausible criminal investigation. However, the confidentiality of SARs was created specifically to reduce to a minimum the circumstances under which a suspect would be able to take legal or other (e.g. violent) action against the reporting entity or individuals believed responsible for the reports.

Under the Data Protection Act 2018 (DPA18) and its predecessors, individuals normally can request from an organisation any data held on them within this organisation However under its establishing legislation – the Crime and Criminal Courts Act 2013 – the NCA is exempt from Freedom of Information requests and the FIU would certainly not respond to questions from the public. Section 45(4) DPA18 makes it clear that data controllers have the right to restrict access.

LPP applies to professionals in the legal sector, but they will still have to file a SAR if the privileged information is communicated to them to further a criminal purpose (if they suspect or know this criminal purpose). If they do not do so, they may be committing a money laundering offence, in addition to any other substantive offences.

Under section 40(2) POCA, the Crown Court can make a pre-charge restraint order, but only if it is satisfied that: (a) a criminal investigation has been commenced, and (b) there are reasonable grounds to suspect that the alleged offender has benefited from his criminal conduct. But any restraint order must, under section 41(2A) POCA, contain a legal aid exception. Second, under section 41(7A–C) POCA, a pre-charge restraint order must now "include in the order a requirement for the applicant for the order to report to the court on the progress of the investigation at such times and in such manner as the order may specify (a 'reporting requirement')", unless the Court decides that, in the circumstances of the case, a reporting requirement should not be imposed. However, if the Court so decides, it must give reasons for its decision. Third, the Court must discharge the order if proceedings for the offence are not started within a reasonable time (section 41(7B)(b) POCA), whether or not an application to discharge the order is made. There is active discussion in 2019 of methods by which restraint orders can be incentivised. These are partly an issue of departmental budgets and the caution of prosecutors in risking the costs of applications for restraint or indeed of Unexplained Wealth Orders.

[116] [2012] EWHC 1283.

[117] [2018] EWHC 1843 (QB).

11. Judicial Review or Other Remedies

Suspects cannot be involved in the FIU process. If suspects were to suspect that a SAR had been filed, they can launch litigation. But as the *Shah v HSBC* case (mentioned above) demonstrates, the court is expected to decide in favour of the reporting entity if the SAR has been filed in good faith. *Lonsdale v National Westminster Bank* is a rare exception.

If the suspect were to launch litigation, it would be for the courts to decide whether the FIU has overstepped its authority and treated someone unfairly by passing the SAR to another authority to launch or assist an investigation. Even when an FIU investigation leads to prosecution, FIU material remains confidential as they cannot disclose the source of the SAR.

SIMILAR POWERS OF SUPERVISORY BODIES

12. Financial Supervision

In many fraud cases, the fraud automatically involves money laundering as part of the extraction of the funds. The FCA is an authorised recipient of SAR data, and can investigate the systems and controls of FCA-regulated entities for AML/counter-terrorist financing weaknesses. It can also launch its own criminal investigations, for example into insider dealing and other market conduct offences within its legal competence (regulated entities file reports with the FCA on transactions suspected to be insider dealing). Many such offences involve money laundering, but quite properly, they are unlikely to be labelled as "money laundering cases". In some instances, for example, a report on insider dealing will be done in parallel with a SAR.

It is sometimes a matter of tension as to which body will have the obligation of regulating particular sectors, an issue which has resource implications, especially at a time of austerity. HMRC can regulate sectors such as money service businesses within its legal competence, as well as investigate money laundering suspicions on its own initiative.[118] The staff resource for HMRC's Anti-Money Laundering Supervision team equates to around 200. In the period 2015–17, HMRC staff carried out activities including:[119]

"– Keeping a register of all supervised businesses and publishing a lookup facility on GOV.UK;
- Specifying what information those applying for registration must provide to HMRC.
- Carrying out Fit and Proper tests;
- Requiring information and attendance at meetings of relevant representatives in or connected with the business;

[118] https://www.gov.uk/guidance/money-laundering-regulations-appeals-and-penalties.
[119] HMRC, *Report on Tackling Financial Crime in the Supervised Sectors 2015-2017*, 2018, p. 6.

- Entering business premises – inspecting, observing and making copies of information found there;
- Refusing to register a business;
- Imposing civil penalties for failure to meet any requirement of the regulations.
- Where judged by them to be appropriate, instituting proceedings for criminal offences; and
- Making disclosures to other supervisory authorities."

HMRC is responsible for the supervision of estate agency businesses, high value dealers, money service businesses, and trust or company service providers who are not supervised by the FCA or PBSs. Overall, it supervises 23,619 obliged entities; of these, 1,366 firms and 148 sole practitioners act as Trust and Company Service Providers (TCSPs). In 2018-19, HMRC conducted 107 DBRs and 1,265 onsite visits: so about 6% of HMRC's supervised population was subject to either a DBR or an onsite visit. About half the DBRs and onsite visits led to informal or formal action, but no more details are available on the specifics or on their consequences for future behaviour.

Non-financial Sector Supervision

Supervisory bodies can only probe within the scope of their supervisory mandate. Any case-specific leads are followed by law enforcement/investigative bodies (e.g. the NCA, SFO). Those regulators within the OPBAS mandate may receive SARs,[1279][120] but there may be a tension between investigating disciplinary offences (e.g. non-compliance with solicitors' client or office account rules) and investigating money laundering or other substantive crime cases. Normally, the disciplinary offences would be made subservient to the criminal ones (if the regulatory body is aware of them), but could be pursued as standalone ones or in the aftermath of a conviction. Prosecutions for money laundering are comparatively rare and there is no requirement that

[120] OPBAS aims to improve consistency of professional body AML supervision in the accountancy and legal sectors, but *does not* directly supervise legal and accountancy firms. The professional body AML supervisors overseen by OPBAS that may receive SARs are listed in Schedule 1 to the Money Laundering Regulations, and are as follows: the Association of Accounting Technicians; the Association of Chartered Certified Accountants; the Association of International Accountants; the Association of Taxation Technicians; the Chartered Institute of Legal Executives/CILEx Regulation; the Chartered Institute of Management Accountants; the Chartered Institute of Taxation; the Council for Licensed Conveyancers; the Faculty of Advocates; the Faculty Office of the Archbishop of Canterbury; the General Council of the Bar/Bar Standards Board; the General Council of the Bar of Northern Ireland; the Insolvency Practitioners Association; the Institute of Certified Bookkeepers; the Institute of Chartered Accountants in England and Wales; the Institute of Chartered Accountants in Ireland; the Institute of Chartered Accountants of Scotland; the Institute of Financial Accountants; the International Association of Bookkeepers; the Law Society/Solicitors Regulation Authority; the Law Society of Northern Ireland; and the Law Society of Scotland.
OPBAS *does not* supervise: members of professional bodies, such as firms, accountants and solicitors, or any other type of business subject to the requirements of the Money Laundering Regulations; statutory anti-money laundering supervisors such as the Gambling Commission and HMRC; activity carried out by professional body supervisors outside the UK; and the adequacy of any functions performed by professional body supervisors unrelated to AML supervision – this includes any oversight of their members' controls over other types of financial crime, such as those related to the prevention of fraud, improving data security and the implementation of financial sanctions and asset freezes.

disciplinary offences should reveal their connection with money laundering suspicions. It would usually be easier to pursue them for technical breaches and therefore the true effect of AML provisions in disciplinary cases is obscure. There is no equivalent in the UK of the continental European and Canadian provisions whereby the Bar Association has the mandate to investigate money laundering within their members, as a way of protecting legal confidentiality.

The OPBAS Annual Report for 2019 stated that a year ago, 91% of relevant PBSs were not fully applying a risk-based approach to their supervision. One year on, only 14% are not yet driving supervisory activity by AML risk. They also observed a notable increase in governance arrangements for AML supervision. A year ago, 44% of PBSs lacked clear accountability for their supervisory work. This figure had reached zero by the end of 2019.

Despite these improvements across the industry, OPBAS identified a number of areas for improvement, including:

- More enforcement action where appropriate [though appropriateness is not defined]. 41% of relevant PBSs did not take any kind of enforcement action for AML non-compliance
- Better information and intelligence sharing. 40% of PBSs were not members of established intelligence sharing systems
- Quality assurance of supervisory decision-making, with 32% of PBSs lacking formal procedures.
- Better internal staff training, with 8% of PBSs still in need of structured training

REPORTING OBLIGATIONS OF SUPERVISORY AUTHORITIES

All supervisory bodies[121] for the various parts of the AML-regulated sector should notify the FIU if, in the course of their work, they become aware or suspicious that money laundering or terrorist financing is taking place (or has taken or will take place) at an organisation supervised by them. The extent to which this is actually done is unknown.

REPORTING BY OTHER AUTHORITIES

Other authorities are not part of the regulated sector, but the expectation is that they will notify the FIU if they consider it to be appropriate. This very rarely happens, but they are free to do so. Unlike some other European countries (e.g. the Netherlands), where police-tax authority data sharing is commonplace, there are legal provisions about confidentiality within HMRC by the

[121] According to the Money Laundering Regulations (Part 11: S.103), a long list of public authorities must inform the NCA if they know or suspect or have reasonable grounds to suspect money laundering or terrorist financing.

Commissioners for Revenue and Customs Act 2005 that make it criminal for them to communicate suspicions to other bodies except in particular circumstances via specified gateways.[122]

STATISTICS

13. Number of Reports by Supervisory Authorities and Other Authorities

It is unclear whether and how many SARs may have been filed by supervisory or other authorities. There is no such separate category in the FIU's annual reports, which provide the number of SARs filed per sector. There is also a category of SARs filed by non-AML regulated entities.

14. FIU Analysis

There are no statistics on the number of FIU investigations and the value of transactions associated with these investigations. Nor are there any data on what investigations are conducted on their own initiative by the FIU (though these would normally happen only in collaboration with the NCA or another criminal investigation body). However, there are statistical data in the FIU's annual reports on the amounts seized that are attributed by the NCA to DAML and non-DAML SARs. Thus, the 2019 report[123] proclaims "£131,667,477 denied to criminals as a result of DAML requests (refused and granted) – up 153.66% on the previous year's £51,907,067". This rise is attributable mostly to the recently introduced Asset Freezing Orders in the Criminal Finances Act 2017, which were used more than 650 times in 2018/19 to freeze over £110m of suspected illicit funds – and many more since the start of 2020. First, a senior officer or one authorised by a senior officer can apply to a magistrates' court for an Account Freezing Order where there are reasonable grounds to suspect that the account contains the proceeds of crime or is intended for use in unlawful conduct. This is a low threshold and such orders are routinely granted: hence their popularity compared with more elaborate and expensive mechanisms.

Subsequently, having investigated, the law enforcement agency may then apply for a Forfeiture Order. If the magistrates' court is satisfied that the funds in the account represent the proceeds of crime or are intended for use in unlawful conduct, it will grant a Forfeiture Order. The standard of proof is the balance of probabilities and there is no requirement for a criminal conviction to

[122] See https://www.gov.uk/hmrc-internal-manuals/information-disclosure-guide/idg50000. We note that reports on transactions suspected to be insider trading are filed with the FCA.
[123] P.4.

have been obtained against any party.

Note that these are asset *seizures*, not confiscation, so it is not clear at this point for how long the (variable) period of 'denial' to suspected offenders may be. Proper interpretation of such data requires analysis of the attrition between the alleged predicate crimes, SARs, seizures confiscation orders and actual confiscation. We can expect this to vary over time and between jurisdictions.

V. DATA FLOW AND DATA PROTECTION

From FIU to Private Sector

The FIU does not generally provide data to the private sector. Feedback is provided generally, for example, through seminars and industry communications (e.g. typologies, how to structure SARs better, what level of detail to provide); it is not case-specific, at least in a formal sense. The FIU will not tell the obliged entity what the outcome of a SAR is and whether it provided helpful investigative leads, although if further cooperation from the obliged entity is required on the SAR, the obliged entity may eventually learn about any potential investigation.

Established in 2015 to complement the SAR framework, the JMLIT is a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats. The JMLIT consists of:

- over 40 financial institutions;
- the FCA;
- CIFAS;[124] and
- five law-enforcement agencies: the NCA, HMRC, the SFO, the City of London Police, and the Metropolitan Police Service.[125]

The JMLIT is not used to get feedback on specific SARs; it is a forum used to share information on new typologies, existing vulnerabilities and live tactical intelligence. The authorities, e.g. the NCA, HMRC or SFO, provide leads, from investigations they are working on, to the representatives of the financial institutions that are members of the JMLIT. They, in turn, then search their internal systems to check for any exposure to the subjects of these investigations (e.g. as clients or counterparties in transactions) and provide the results back to the authorities through the JMLIT. Those security-vetted bank staff that are part of the JMLIT can get limited feedback,

[124] CIFAS is a fraud prevention service in the UK. It is a not-for-profit membership association representing organisations from across the public, private and voluntary sectors. See https://www.cifas.org.uk.
[125] See https://nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre.

in certain circumstances (e.g. if it comes to issuing a freezing order) where they are working on a joint investigation, but that information is classified and is not more widely distributed.

From Private Sector to FIU

In terms of personal data, there is no limit as to what and how much information is provided by the obliged entity to the FIU, as long as this is for financial crime prevention purposes and the data are relevant to the suspicious (or suspected) activity.[126] One of the FATF-praised initiatives of the JMLIT process is to generate "super-SARs", which combine data from several institutions, and this approach is expected to expand using the gateway provisions.

DATA EXCHANGE BETWEEN FIU AND TAX AUTHORITIES

1. From FIU to Tax Authorities

As discussed above, HMRC has direct access to the FIU's data (except for certain sensitive categories such as terrorist financing data).

2. From Tax Authorities to FIU

HMRC will provide information to the FIU to the extent that it helps the FIU search its database for further SARs relevant to HMRC's case. However, there has been criticism of past unwillingness of HMRC to pass on information to the FIU or to the intelligence agencies about tax suspects later demonstrated to have terrorist connections.[127] Such issues need to be understood in the context of organisational culture rather than purely in terms of legal gateways.

Further, as per the FATF's UK Mutual Evaluation Report, "HMRC databases, including the register of trusts with UK tax consequences (Trust Registration Service), tax information, and information on UK citizens with overseas bank accounts may be accessed directly by the HMRC's law enforcement arm and are available to other LEAs [law enforcement agencies] upon request."[128] There are dedicated HMRC officers seconded to the FIU to manage this process, but they only have indirect access to the FIU.

---

[126] There may be client privilege limitations, but that is different from personal data limits. With regard to the FIU requesting data, this can only happen as a follow-up to a SAR, not prior to a SAR. The FIU does not have investigative authority in that sense. But another body can request information, for instance the FCA, the NCA (where the FIU sits), the SFO, etc.

[127] "Sunbed boss 'linked to £8bn fraud that helped bin Laden'", Sunday Times, 14 April 2019. https://www.thetimes.co.uk/article/sunbed-boss-linked-to-8bn-fraud-that-helped-bin-laden-kkldskl8r.

[128] FATF, *Mutual Evaluation Report – UK*, 2018, p. 44.

The Mutual Evaluation Report also states on cash declarations:

> "Criterion 32.6 – Cross-border cash declarations which are reported to HMRC are provided to the NCA on a monthly basis under an MOU between the agencies which has been in place since 22 January 2018, with the first exchange of information under the MOU in February 2018. This information can then be provided to the UKFIU, but there are limitations as to what data can be stored in line with the Operating Procedure for dealing with Bulk Personal Data. This data can also be accessed by HMRC secondees to the UKFIU."[129]

According to the 2019 amendments to the Money Laundering Regulations, where the NCA has, in its performance of FIU functions, disseminated any information to a United Kingdom competent authority, that authority must, upon request, provide a report to the NCA about the authority's use of that information, including the outcome of any investigations or inspections conducted on the basis of that information.

INFORMATION FLOW BETWEEN FIU AND FOREIGN COUNTERPARTS

If there is a Memorandum of Association (which typically is put in place in accordance with the Egmont Group's standards), the UK's FIU can share information with foreign FIUs, including personal data, to the extent this is relevant to preventing and disrupting crime.

The UK Mutual Evaluation Report noted that:

> 494. The UK generally has good access to basic and BO information … and can provide this information to foreign jurisdictions in a timely manner upon request. However, foreign LEAs may be directed to the public PSC register for BO information, whereas UK LEAs would typically corroborate this information with BO information from financial institutions and DNFBPs where available … Where the information is not available from the PSC register, the UK can provide assistance using other sources …
>
> 495. The UK authorities advised that foreign requests for basic and BO information on legal persons/arrangements are common. Where relevant, the UKFIU and certain LEAs will direct requests for information on legal persons to the public PSC register. In doing so, the requesting agency is not advised that to obtain *verified* BO information it is necessary to seek such information from the relevant FI or DNFBP via a request for formal or informal co-operation. This may result in authorities relying on unverified information (see Chapter 7 on IO.5).
>
> 496. Where the requested information is not publicly available on the PSC register, it can be obtained through a request to Companies House (for information on legal persons), to HMRC (for

[129] Ibid, p. XX.

information on trusts), or to the relevant LEA (for information held by FIs or DNFBPs where available). These requests can generally be answered in a timely fashion, with non-urgent requests to Companies House and financial institutions typically receiving a response within two weeks."[130]

In 2016 the UK entered into an agreement with three Crown Dependencies and six Overseas Territories (subsequently increased to eight) with financial centres to enhance the sharing of company beneficial ownership information on a bilateral basis. The Crown Dependencies and Overseas Territories agreed provide LEAs, including tax authorities, with beneficial ownership information of companies registered in their jurisdiction within 24 hours (or, where urgent, within an hour).[131]

Excluding general and informal requests, the inwards and outwards data flow is captured in the following UK FIU data,[132] over half of which may be reduced post-Brexit unless it is re-routed via the Egmont Group and CARIN:[133]

Table 3. Number of financial intelligence requests received and made by the UK FIU, 2018-19 (2017-18 data in brackets)

	Number of financial intelligence	Number of financial intelligence requests made by UK's FIU
Egmont network	1,132 (742)	1,147 (665)
FIU.Net network (EU)	234 (472)	114 (544)
ARO network	244 (224)	227 (311)
CARIN network	29 (17)	30 (39)
Total	**1,639 (1,455)**	**1,518 (1,559)**
Intelligence reports spontaneously received from overseas		1,295 (1,621)
Intelligence spontaneously disseminated (excluding Europol)		399 (470)

[130] Ibid, p. XX.

[131] Home Office, *Statutory review of the implementation of the exchange of notes on beneficial ownership between the united kingdom, crown dependencies and overseas territories*, United Kingdom, June 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/812355/Statutory_review_of_the_exchange_of_notes_arrangements.pdf. The number has subsequently increased.

[132] *Suspicious Activity Reports (SARs) Annual Report 2019*, p. 6. *Suspicious Activity Reports (SARs) Annual Report 2018*, p. 4.

[133] The ARO network, which is within the EU, and the CARIN network, which is worldwide but has Europol as its secretariat, are networks (both mentioned in the table) of asset recovery offices (see https://eucrim.eu/articles/asset-recovery-uncac-convention-possibilities-and-limitations/). As such, it would appear safe to assume that the numbers relating to the Egmont network and the FIU.Net network are FIU-to-FIU requests, while the rest are not necessarily.

Source: National Crime Agency.

According to the 2019 amendments to the Money Laundering Regulations:

"3. The NCA must take such steps as it considers appropriate to co-operate with foreign FIUs in their performance of FIU functions.

Provision of information in response to external requests

4. In response to an external request, the NCA must (subject to paragraph 10) provide promptly any relevant information in the NCA's possession.

5. Where an external request is received and the NCA does not possess information which the NCA considers relevant to the external request, and it suspects a relevant person possesses such information, the NCA-

a) may exercise its powers under Parts 7(3) and 8(4) (investigations) of the 2002 Act, any orders made under section 445(5) (external investigations) of that Act, or Part 3 of the 2000 Act(6), as applicable, to seek an order for information from such person, and

b) must (subject to paragraph 10 [see restrictions below]) provide any relevant information received in consequence of any such order promptly to the foreign FIU concerned.

6. The NCA must designate at least one point of contact with responsibility for receiving external requests.

7. Where the NCA has provided relevant information to a foreign FIU, and that foreign FIU makes a request for consent to disseminate some or all of the relevant information to a foreign competent authority, the NCA must (subject to paragraph 11 [see restrictions below]) consent to the dissemination of as much of the requested information as possible and communicate its consent promptly to the foreign FIU.

8. Where the NCA provides relevant information in response to an external request in accordance with this Schedule, the NCA shall take such steps as it considers appropriate to ensure that such information is transmitted securely."

The 2019 amended regulations include these conditions and restrictions on provision or further dissemination of relevant information:

"9. The NCA may impose such restrictions and conditions on the use of relevant information provided in response to an external request as the NCA considers appropriate.

10. Where an obligation arises under this Schedule for the NCA to provide relevant information in response to an external request, the NCA may decide not to provide some or all of the information where and to the extent that the NCA considers that doing so could be contrary to national law.

11. The NCA is not required to comply with the duty to give consent to the dissemination of information to a foreign competent authority under paragraph 7 if and to the extent that the NCA considers that the giving of such consent could—

(a) prejudice an investigation, whether into a criminal cause or matter or in relation to any investigation referred to in section 341 (investigations) of the 2002 Act(7) or to which Schedule 5A (terrorist financing investigations) to the 2000 Act(8) applies; or

(b) be contrary to national law.

12. The NCA must have particular regard—

(a) where making a decision under paragraph 10, to the need for as unfettered an exchange of relevant information in response to external requests as possible, or

(b) where making a decision under paragraph 11, to the need for as unfettered dissemination of information as possible by a foreign FIU to foreign competent authorities, in order for the foreign FIU concerned to carry out FIU functions efficiently and effectively."

Restrictions on Data Transfer from FIU to Foreign FIUs

See section above. The DPA18 covers the processing of personal data:

- within and outside the scope of the GDPR;
- by competent authorities for law enforcement purposes; and
- by the intelligence services.

Personal data can only be transferred outside the EEA if adequate protections are in place (e.g. contractual clauses) or if the country to which the data is being transferred is deemed "adequate".

On the above basis, in terms of data protection, different requirements will apply depending on whether the foreign FIU is in the EU or outside the EU. Within the EU the authorities will have to apply EU data protection legislation (the GDPR), EU FIUs and other relevant bodies (including

Europol) are considered to adhere to an equivalent standard.[134] Exchanging information with a non-EU FIU is more challenging. But ultimately, the flow of information will depend on whether there is a signed MOU and what its terms are. The Egmont Group is attempting to develop inter-FIU SARs sharing on an international basis.

According to section 10(5) DPA18, processing personal data relating to criminal convictions and offences must meet certain conditions, such as the processing being necessary to make a disclosure in good faith under section 339ZB POCA, to detect or prevent illegal acts (paragraph 10, Schedule 1 DPA18), or to comply with or assist others to comply with a regulatory requirement that involves taking steps to establish whether a person has committed an illegal act (paragraph 12, Schedule 1 DPA18).

Restrictions on Use of Data Obtained from Foreign FIUs

As explained above, the general data protection and privacy laws apply. It will also depend on the relationship between the two countries (e.g. within or outside the EU, as explained above) and whether there is a MOU and its terms.

According to the amended Money Laundering Regulations of 2019, where the NCA receives information from a foreign FIU, the NCA must:

(a) use the information only for the purpose for which it was sought or provided, unless it has obtained the prior consent of the foreign FIU to any other use of the information;

(b) comply with any restrictions or conditions of use which have been imposed by the foreign FIU in respect of the information; and

(c) obtain the prior consent of the foreign FIU to any further dissemination of the information.

EVIDENTIAL VALUE OF FIU-GENERATED DATA IN COURT PROCEEDINGS

SAR data, generally, cannot be used directly in court proceedings as that would mean disclosing the source of information. In a 2018 case, for the first time, courts allowed the subject of a SAR to see the SAR. This was in *Lonsdale v National Westminster Bank*.[135] David Lonsdale, a barrister, told

[134] FIU.Net became operational in 2002 (under Council Decision 2000/642/JHA). In January 2016, FIU.Net was incorporated into Europol. Article 5.4 of the aforementioned Decision stipulates that FIUs "shall undertake all necessary measures, including security measures, to ensure that information submitted under this Decision is not accessible by any other authorities, agencies or departments" than those it is intended for. The extent to which FIU.Net will become a truly fluid pan-EU financial intelligence facility is not currently known. It is doubtful that this UK access will survive Brexit.

[135] [2018] EWHC 1843 (QB).

the media that he had seen the SARs following the court decision, but that the terms of the settlement meant he could not say what they contained. He further stated:

> "Money coming into my bank accounts came from transparent and lawful sources, that is to say my rental property and my practice at the Bar. The bank was perfectly well aware of the source of this money. The bank never sought to provide any justification for freezing my accounts and writing to the NCA. It just relied upon a claim that it suspected that money was the proceeds of crime but could not tell me why as this was all 'confidential'."[136]

However, SARs are used for investigative leads and to that extent, indirectly, they can contribute to court proceedings. The UK court disclosure rules require that undisclosed material which contributes to the case must be disclosed to the defence to allow them to develop a defence based not only on the prosecution (or civil plaintiff) case. However, since the SARs, as financial intelligence, are essentially leads, it is the material discovered based on these leads that is disclosed: otherwise the SARs themselves would be disclosed, which is contrary to policy.

The FIU seldom develops its own investigations, and approved financial investigators do so but are attached not to the FIU but to police or other non-police enforcement agencies.

If any non-public information in a SAR is to be used, due process must be followed in order for the information to be admissible in court; for example, the obliged entity that had made the disclosure must first provide consent and, as described above, client privileged information cannot be used; further information requests must be based on a magistrates' court order. This, however, is not tested.

DATA SHARING BETWEEN OBLIGED ENTITIES REGARDING SARs AND FIU REQUESTS

3. Data Sharing Inside a Group

Such sharing inside a group is possible, within a GDPR framework agreement, if necessary to detect and prevent crime. It is now explicitly stated in the amended 2019 Money Laundering Regulations that a group's policies, controls and procedures for data protection and sharing information for the purposes of preventing money laundering and terrorist financing with other members of the group must include policies on the sharing of information about customers, customer accounts and transactions. This may yet give rise to problems with branches or legally separate institutions of the group in financial secrecy jurisdictions.

---

[136] Neil Rose, "Barrister wins right to see reports his bank made to police", Legal Futures, 10 October 2018, https://www.legalfutures.co.uk/latest-news/barrister-wins-right-to-see-reports-his-bank-made-to-police.

4. *Data Sharing with Similar Professions*

The Criminal Finances Act 2017 introduced important changes to the AML regime for the reporting of suspicious activity under Part 7 POCA. A change that had a significant practical impact on lawyers, estate agents and financial sector professionals is the ability for regulated persons to share information relating to a money laundering suspicion. Section 11 of the Criminal Finances Act 2017 inserted sections 339ZB–339ZG into POCA, which enable regulated persons to request and share information with their regulated peers. Any sharing of information will be voluntary. This sharing is relevant to the SAR process to the extent that it can help improve the quality of SARs, as financial institutions can build more clarity around certain events by communicating with each other.[137] Insulation from resulting claims of breach of confidence or contravention of data protection laws is ensured by section 339ZF POCA, which provides that a relevant disclosure "made in good faith" does not breach any duties of confidence or any other restriction on information disclosure. If information is shared, the new framework then contemplates a joint SAR being made. But see above regarding client privileged information. Information can only be disclosed if four key conditions are met: (a) the person making the request and the would-be discloser must be regulated;[138] (b) the information must have been obtained in the course of regulated business; (c) the FIU (which is within the NCA) must have been properly notified of the information to be disclosed; and (d) for the information to be disclosed, the would-be discloser must be satisfied that it "will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering".[139] There are grounds for scepticism about how frequently these provisions will be used and therefore will have practical as well as symbolic importance.

As discussed previously, according to section 10(5) DPA18, the processing of personal data relating to criminal convictions and offences must meet certain conditions: these include the

---

[137] Obliged entities from the same group can also share intelligence for financial crime prevention purposes within a GDPR framework agreement.

[138] Intelligence can be shared in this form not only upon request but also where one obliged entity shares with another to prevent financial crime. Both must be obliged entities.

[139] The threshold for the sharing of information is very low. Any number of personal details in a business's possession, such as a client's former name, family details, historical transactions or names of their business interests could well assist in determining a matter relating to a money laundering suspicion even if, in isolation, those details do not appear very useful. See the Home Office circular, "Money laundering: sharing of information within the regulated sector", https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/679032/HO_Circular-_Sharing_of_information_within_the_regulated_sector_1.0.pdf. In this context, in relation to point (c) we add that by sharing information, regulated entities may determine that actually there were no valid grounds for a SAR, which means that in retrospect, the FIU had been notified for no good reason (which just adds to the clutter they need to deal with). If, on the other hand, the shared information results in better analysis and a joint SAR, then that (rather than a notification based on uncertain facts) is what the FIU needs to see.

processing being necessary to make a disclosure in good faith under section 339ZB POCA (i.e. an obliged entity can request information about a suspect from another obliged entity), to detect or prevent crime (paragraph 10, Schedule 1 DPA18) or to comply with or assist other persons to comply with a regulatory requirement that involves taking steps to establish whether a person has committed an illegal act (paragraph 12, Schedule 1 DPA18).

Separate to the SAR process, financial institutions are allowed to share information under strict terms through the JMLIT.[140] There are questions about the scalability of this process, which depends also on trust between members, but it has been heralded by the FATF and by some jurisdictions (e.g. Singapore and Hong Kong).[141]

5. *Data Sharing with Obliged Entities Outside the EU*

The above-discussed data sharing provisions (see section 2 above) apply to entities that are AML-regulated in the UK. Data relating to SARs cannot be shared with entities in other countries unless they are part of the same organisation – a group – *and* data are shared for the purposes of crime prevention and detection (UK-headquartered obliged entities are expected to have a group-wide compliance programme, although this does not necessarily mean that identical processes are applied everywhere – an issue raised in some of the FinCEN leaks cases). However, even in this instance, the organisation must adhere to data protection laws. This means that while within the EU there are shared GDPR standards, outside of the EU data can be shared only with parts of the organisation that are in GDPR-equivalent jurisdictions within a GDPR framework agreement.

VI. BENEFICIAL OWNERSHIP TRANSPARENCY

BENEFICIAL OWNERSHIP INFORMATION

1. *Scope and General Framework*

a. General Framework

The Companies Act 2006, the People with Significant Control Regulations 2016 and Parts 5 and 6 of the Money Laundering Regulations 2019 contain provisions relating to beneficial ownership. Any entity registered in the UK must disclose its beneficial owners through documentation filed with Companies House (the UK's company registry). A beneficial owner, also known as a person

[140] https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre.

[141] For a positive perspective, see Nick Maxwell (2020) *Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'*, RUSI.

with significant control (PSC), is anyone in the company who meets one or more of the conditions listed in the People with Significant Control Regulations 2016, which applies to registered and unregistered companies, societates Europaeae, limited liability partnerships and eligible Scottish partnerships (Scottish limited partnerships and Scottish qualifying partnerships).[142] A company can have more than one beneficial owner. Once a company has identified its PSCs, it needs to record their details in its own PSC register and inform Companies House.[143]

The information it must obtain, confirm and enter in the company's own PSC register will depend on whether the PSC is a person or a registrable relevant legal entity (RLE). Where it is a RLE within the PSC regime, other than the RLE's ownership, there is no need for the entire ownership chain to be reflected in files as the RLE's ownership should be reflected in the RLE's own PSC statement. Where the legal entity is outside the PSC regime (e.g. registered offshore), then its ultimate ownership must be reflected in the subject company's PSC register.

If, for some reason, the PSC information cannot be provided, other statements will need to be made instead to explain why the PSC information is not available. The register can never be blank.

Information on the company's register and on the PSC register at Companies House must be kept up to date. New information must be entered onto the register within 14 days.

b. Definition of "Beneficiary" and "Effective Control"

The definition of ultimate beneficial owner/PSC is based on the EU directives. In the context of PSC,[144] a beneficial owner is a person who:

- holds, directly or indirectly, more than 25% of the shares;
- holds, directly or indirectly, more than 25% of the voting rights;
- holds the right, directly or indirectly, to appoint or remove a majority of directors;

[142] Department for Business, Energy and Industrial Strategy, "Register of People with Significant Control", June 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/753027/170623_NONSTAT_GU_1_.pdf

[143] Companies to which Chapter 5 of the FCA's Disclosure and Transparency Rules (DTR5) applies are subject to these requirements, as DTR5 (which deals with disclosure of voting rights) already requires disclosure of major shareholdings to the market, including interests that are held indirectly. UK-incorporated companies with shares listed in London or another EEA regulated market or on specified markets in Switzerland, the USA, Japan and Israel are exempt since they already have to disclose detailed ownership information under the EU Transparency Directive or similar transparency rules. However, all other UK-incorporated companies (including UK-incorporated subsidiaries of UK Main Market and AIM companies) will be required to maintain a PSC register.

[144] ML Regulations - "beneficial owner" of a non-listed corporate means: (a) any individual who exercises ultimate control over the management of the body corporate; (b) any individual who ultimately owns or controls (in each case whether directly or indirectly), including through bearer share holdings or by other means, more than 25% of the shares or voting rights in the body corporate; or (c) an individual who controls the body corporate.

- otherwise has the right to exercise, or actually exercises, significant influence or control over the company; or
- has the right to exercise, or actually exercises, significant influence or control over the activities of a trust or firm which is not a legal person, the trustees or members of which would satisfy any of the four conditions above.

Most small companies' PSCs are likely to fall into the first and second, and possibly the third, categories above. The fourth and fifth categories are typically associated with more complex corporate structures.

c. Definition of "Information"

"Information" in the sense of "personal data" – considering Regulation (EC) No 45/2001 - is defined in data protection legislation as any information relating to an identified or identifiable natural person.

2. Special Rules for Entities with a Cross-border Dimension

Entities may be able to share information between branches in different countries, subject to data protection laws that may inhibit this. There are no special rules, since the UK cannot force companies to break the secrecy laws in their other places of business. This can be a source of tension.

BENEFICIAL OWNERSHIP REGISTRIES

3. Scope and General Procedure

Companies registered in the UK are required to disclose their beneficial ownership through a centralised government company registry, Companies House.

4. Ex ante *Verification of Accuracy*

The information is entered into the company registry based on documents provided by the company. The information entered is checked against the original documents and companies are required to provide accurate information. The Companies Act 2006 sets out the criminal offence of providing false information on the company register. In 2018, the first company director was successfully prosecuted for falsifying company information under this law. He was ordered to pay over £12,000 after he pleaded guilty to filing false information on the UK's company

register.[145] However, this prosecution attracted severe criticism because the person convicted was aiming to expose the absurdity of the lack of controls over the quality of filing information and had made no secret of this, intentionally using an absurd name.

Late filing penalties were introduced in 1992 to encourage directors of companies to file their accounts and reports on time, because this information is required for the public record. All companies – private or public, large or small, trading or non-trading – must send their accounts and reports to Companies House every year. If company accounts and reports are submitted late, the law imposes an automatic penalty. The period allowed for filing a company's accounts depends on whether the company is filing its first accounts since incorporation or subsequent accounts.[146]

Failure to file confirmation statements, annual returns or accounts is a criminal offence that can result in directors being fined personally in the criminal courts. Failure to pay the late filing penalty can result in enforcement proceedings. Any criminal proceedings taken as a result of non-filing of confirmation statements, annual returns or accounts is separate from, and in addition to, any late filing penalty imposed against the company for filing accounts late. There is no late filing penalty imposed on confirmation statements or annual returns that have been filed late. The registrar may also take steps to strike the company off the public record if these documents are delivered late.[147]

However, the company registry currently does not vet or seek to verify that the individuals identified as owners in the company's documentation are indeed its true owners. Though the study is now a decade old, in 2008, an independent study found that a large number of individuals featuring as company directors in the UK were disqualified directors or linked to risk in some other way.[148] In September 2020, HM Government announced significant reforms of this passive approach, which coincided with the FinCEN leaks but was not caused by them.

Ex post Review of Accuracy

---

[145] Companies House Press Release, "UK's 'first ever' successful prosecution for false company information", 23 March 2018, https://www.gov.uk/government/news/uks-first-ever-successful-prosecution-for-false-company-information

[146] https://www.gov.uk/government/publications/late-filing-penalties/late-filing-penalties. In 2014/15, the number of penalties issued in England and Wales stood at 165,000, with a total value of around £78 million. However, in 2017/18 the number had reached 204,000. with a cost to businesses of around £87m. See James Bunney, "Late filing of annual accounts up 23% since 2014", Accountancy Daily, 26 September 2018, https://www.accountancydaily.co/late-filing-annual-accounts-23-2014.

[147] https://www.gov.uk/government/publications/late-filing-penalties/late-filing-penalties.

[148] Antony Savvas, "UK Companies House register contains 3,994 high-risk individuals, Datanomic finds", Computer Weekly, 21 February 2008, https://www.computerweekly.com/news/2240085116/UK-Companies-House-register-contains-3994-high-risk-individuals-Datanomic-finds.

See comments in the previous section. Global Witness has reviewed the data and concluded:[149]

" – Almost 3,000 companies listed their beneficial owner as a company with a tax haven address – something that is not allowed under the rules. There are problems with how the data has been inputted. For example, you can write anything in the nationality field and we found over 500 ways of putting 'British', including ten people who wrote 'Cornish'.
– 76 beneficial owners share the same name and birthday as someone on the U.S. sanctions list. We have to do more digging to find out whether these are actually the same people, but it's an insight into what is possible with this new information.
– Most beneficial owners are from the UK, followed by a number from other European countries and India and China."

According to 2019 amendments to the Money Laundering Regulations, obliged entities must report to the company registry discrepancies they see between beneficial ownership information available to them and company registry records. How active they are required to be in seeking out potential discrepancies is not yet resolved.

ACCESS TO BENEFICIAL OWNERSHIP INFORMATION

5. *Access by FIU and Other Authorities*

The information filed with Companies House is a matter of public record. All information that appears on the register can be accessed by the public. In 2016 the UK, three Crown Dependencies and six British Overseas Territories committed to enhance the effectiveness of sharing company beneficial ownership information on a bilateral basis between the UK and the Crown Dependencies and major Overseas Territories.[150] They agreed to provide law enforcement agencies with this information on request for companies (also referred to in the agreements as "corporate and legal entities") incorporated in their respective jurisdictions. These arrangements were called the Exchange of Notes (EoN) for Information Sharing and came into force on 1 July 2017.

[149] Robert Palmer and Sam Leon, "What does the UK beneficial ownership data show us?", Global Witness blog, 22 November 2016, https://www.globalwitness.org/en/blog/what-does-uk-beneficial-ownership-data-show-us/.
[150] The number of overseas territories expanded to eight in 2020: for a ministerial statement, see HLWS361 (15 July 2020).

A Statutory Review was required by section 445A POCA, as amended by section 9 of the Criminal Finances Act 2017, to assess the effectiveness of the arrangements. It covers the period from 1 July 2017 to 31 December 2018.[151]

The key findings of this Review are:

> "– UK Law Enforcement Agencies (LEAs) report that the EoN has been extremely useful in accessing the information needed to support ongoing investigations.
> – This process gives UK LEAs rapid access to beneficial ownership information on over half a million entities based in the 3 CDs and 6 participating OTs. This represents 87% of businesses in scope of the scheme. Plans are in place for this to reach 100% by December 2020. In addition, these jurisdictions have reciprocal access to information on 3.8 million UK entities through the UK's People with Significant Control public register.
> – During the first 18 months of operation, 296 requests were made. Nearly all of these were originated by UK law enforcement agencies and 118 asked for multiple pieces of information in a single request. This equates on average to nearly 4 requests per week. Responses were provided for all requests made and all but 4 were provided within the agreed time frame."

6. *Access by Obliged Entities*

Companies must identify the PSCs and record their details with Companies House. As per Companies House's website, a PSC is someone who owns or controls the company, also called "beneficial owners". More specifically, as explained on the website of Companies House:

> "A PSC must meet one or more of the following conditions of control.
>
> Most PSCs are likely to be people who hold:
>
> – more than 25% of shares in the company
> – more than 25% of voting rights in the company
> – the right to appoint or remove the majority of the board of directors
>
> If a PSC holds more than 25% of shares, they are likely to hold the same amount of voting rights.
> …

[151] *Statutory review of the implementation of the exchange of notes on beneficial ownership between the United Kingdom, Crown Dependencies and Overseas Territories,* 2019.

> Your PSC might influence or control your company through other means. This could be directly, or on behalf of someone else. For example, someone who tells the directors or shareholders what to do."[152]

This information is filed with Companies House and is accessible to the public, including obliged entities. The register for trusts is not public.

NON-FINANCIAL BENEFICIAL OWNERSHIP REGISTRIES

Regulated entities must collect KYC data including beneficial ownership (e.g. real estate agents on real estate). But this information will not be public. The Land Registry contains information on real estate ownership but if a property is owned by a *company*, not directly by *individuals*, the beneficial ownership is not disclosed in records held by the Land Registry. UK authorities are taking steps to introduce more transparency in this regard in the property sector. Bank vault storage is also subject to KYC, and this will be strengthened by the 5AMLD implementation.

VII. SANCTIONS

SANCTIONS FOR MONEY LAUNDERING

1. Requirement of a Conviction for a Predicate Offence

There can be a standalone prosecution and conviction for money laundering as long as there is at least circumstantial evidence, i.e. it can be inferred (e.g. from the suspect's lifestyle) that the subject of laundering is a benefit derived through criminal conduct. This is set out also in the UK Mutual Evaluation Report 2018, though the statistics of standalone cases are mixed together with those where money laundering is the principal charge (i.e. cases where the launderer is different from the predicate offender).[153] Moreover, based on the case cited in the MER as an example of a standalone prosecution, it is difficult to assess to what extent law enforcement bodies and prosecutors actually benefit from the standalone prosecution provision.[154] The MER also notes that there are yet no statistics on high-end money laundering prosecution and convictions,

---

[152] Companies House, "People with significant control (PSC): who controls your company?", 20 February 2018, https://www.gov.uk/government/news/people-with-significant-control-psc-who-controls-your-company.

[153] The MER states: "UK authorities demonstrated their ability to prosecute and obtain convictions for a full range of ML cases, including stand-alone and self-laundering, third-party laundering and the laundering of foreign predicates." But, according to the report, statistics provided by the UK authorities cannot be disaggregated based on the type of ML pursued.

[154] "The defendant in this case, Katchi, was a collector for an organised criminal group operating throughout the UK. During a traffic stop, Katchi was found to be in possession of large amounts of cash, with further quantities found at his residence upon a search. Katchi was charged with two counts of ML, and received a sentence of six years' imprisonment." FATF, *Mutual Evaluation Report – UK*, 2018, p. 67.

although the number of ongoing investigations is "positive". It is unclear what criteria are used to assess high end other than professional status or case size: an important issue for Canada also.

2. Forms of Sanctions

Under POCA (sections 327-329), the three principal money laundering offences (the concealing offence, the arranging offence, and the acquisition, use and possession offence) are very serious, carrying a maximum of 14 years' imprisonment and/or an unlimited fine (POCA, section 334):

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

(b) on conviction on indictment, to imprisonment for a term not exceeding 14 years or to a fine or to both.

For the ancillary offences of tipping off and failure to disclose (sections 330-332 of POCA) a person is liable (section 334 of POCA):

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both, or

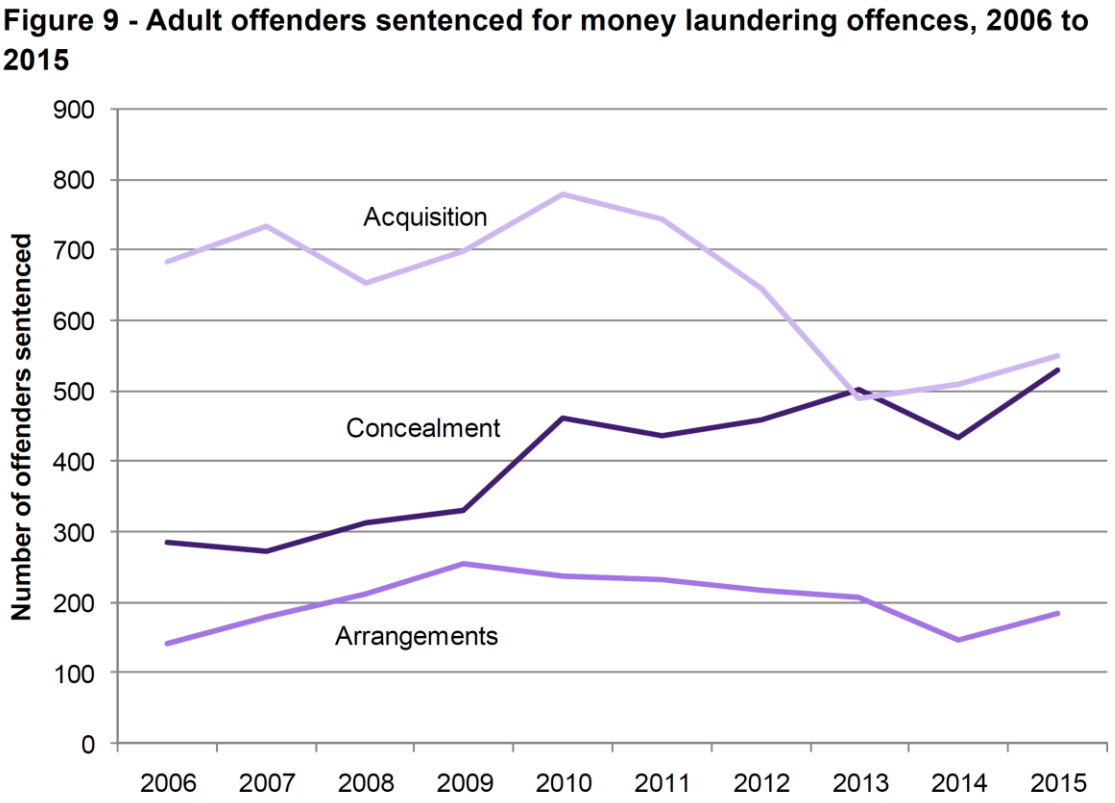
(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

The principal money laundering offences potentially carry heavier penalties than most predicate offences. Theft, for instance, carries seven years.

The Money Laundering Guideline issued by the Sentencing Council for England and Wales[155] covers three offences with the same statutory maximum of 14 years' custody. The lowest volume of the three offences (the "arrangements" offence) showed no clear trend in volumes over the period 2006–2015 (see Figure 1), with 190 offenders sentenced in 2015. The offence of "concealment" saw a gradual increase, reaching 530 offenders sentenced in 2015. Volumes for the offence of "acquisition" increased to 780 offenders sentenced in 2010, but then dropped sharply in 2013, with 550 offenders sentenced in 2015.

[155] Sentencing Council, *Assessing the impact of the Sentencing Council's Fraud, Bribery and Money Laundering Definitive Guideline*, 2018, pp. 15-16. According to the Coroners and Justice Act 2009, a court must follow any relevant sentencing guidelines, unless it is contrary to the interests of justice to do so. The newly created Scottish Sentencing Council has not yet developed such guidance.

Figure 1. Adult offenders sentenced for money laundering offences, 2006–2015



Source: Sentencing Council, 2018, *Assessing the impact of the Sentencing Council's Fraud, Bribery and Money Laundering Definitive Guideline*, p. 6.

In terms of prosecution approaches, the CPS's website gives advice on the use of discretion, which feeds into the sentencing decisions above, because what is not prosecuted cannot be sentenced:

> "– A money laundering charge ought to be considered where the proceeds are more than *de minimis* in any circumstances where the defendant who is charged with the underlying offence has done more than simply consume his proceeds of crime.
> – A charge under section 329 of possession of laundered proceeds, however, may not be necessary, for instance where proceeds were simply 'kept under the bed'. An application for confiscation of the actual benefit of the offence may be sufficient in those circumstances.
> – Where, however, there is any significant attempt to transfer or conceal ill-gotten gains money laundering should normally be considered as an additional charge, in part because the purpose of the concealment will be to defeat or avoid prosecution and confiscation.

– A careful judgement will need to be made as to whether it is in the public interest to proceed with the money laundering offence in the event of a plea to the underlying criminality by a defendant who is also indicted for laundering his own proceeds. The prosecutor should take into account whether the laundering activity involves such a significant attempt to conceal ill-gotten gains that a court may consider a consecutive sentence. Prosecutors should not simply proceed with a money laundering charge in this situation to trigger the lifestyle assumptions in respect of convictions for money laundering under S.327 or S.328. To do so, for no other reason, could attract abuse of process arguments."

In 2015–16, HMRC achieved 30 convictions for POCA money laundering or money laundering-related regulatory offences, resulting in total custodial sentences of 1,033 months.[156] In the same period, using the confiscation and cash forfeiture powers in POCA, HMRC recovered £26.9 million of criminal proceeds, of which £6.5 million was associated with money laundering. In 2016–17 HMRC, achieved 42 convictions for POCA money laundering or money laundering-related offences, resulting in a sum of custodial sentences of 1,115 months. It recovered £24.9 million, of which £6.2 million was associated with money laundering.[157]

HMRC will charge up to £1,500, as well as the penalty for breaches of the Money Laundering Regulations, for failures in relation to, for example:

– CDD;
– risk assessment;
– policies, controls and procedures; or
– record keeping.

HMRC will charge up to £350, as well as the penalty, for failures to, for example:

– register;
– tell HMRC of changes to the business; or
– provide information.[158]

These penalty sums are not very substantial.

A person convicted of one of the "failure to disclose" offences (under sections 330, 331 or 332 POCA) can be subject to criminal prosecution or regulatory censure. On indictment to the Crown

[156] This is a problematic and unilluminating way of representing penalties, as it does not tell us about their distribution, but there is no way of disentangling the official data. It is presumably aimed at producing an apparently large total amount to deter. Its impact on the potential offender population is unknown.
[157] HMRC, *Report on Tackling Financial Crime in the Supervised Sectors 2015–2017*, 2018, p. 10.
[158] https://www.gov.uk/guidance/money-laundering-regulations-appeals-and-penalties.

Court, that person would be liable to imprisonment for a term not exceeding five years or to an unlimited fine or to both.

A person guilty of an offence of tipping-off is liable following conviction on indictment to imprisonment for a term not exceeding two years and/or a fine. For offences committed in England and Wales on or after 12 March 2015, there is no upper limit to the fine that the magistrates can impose.

A person guilty of an offence of prejudicing an investigation is liable on conviction on indictment to a maximum prison term of five years and/or to an unlimited fine.[159]

Where the record keeping obligations under the Money Laundering Regulations are not observed, a firm or person is open to prosecution, including imprisonment for up to two years and/or a fine, or regulatory censure.

In regard to legal entities, there is a range of remedial actions and sanctions. FATF's 2018 MER states that "criminal liability and proportionate, dissuasive sanctions apply to legal persons convicted of ML, without prejudice to the criminal liability of natural persons. Legal persons are punishable by an unlimited criminal fine (POCA, ss.327-329, 334; Interpretation Act 1978, sch.1)."

FATF's 2018 MER notes: "Supervisors use a range of remedial actions to encourage compliance. The three statutory supervisors, FCA, HMRC and the Gambling Commission, have demonstrated their ability to sanction individuals in addition to corporations." For instance, the FCA has a range of remedial actions including:

a) the use of action plans

b) attestations by firms that required improvements have been completed, and

c) early interventions using power under s.166 of the FSMA to require a firm to engage the services of Skilled Person to carry out a review and provide a report to the FCA.

FCA's sanctions include:

a) restricting or suspending a firm's business or licence on either a voluntary basis by the firm or through the use of the FCA's powers to require the business or licence restriction

b) prohibitions, banning individuals from an industry

[159] "Money laundering under the Proceeds of Crime Act 2002 – overview", https://www.lexisnexis.com/uk/lexispsl/corporatecrime/document/391421/55KB-9471-F188-N12W-00000-00/Money_laundering_under_the_Proceeds_of_Crime_Act_2002_overview#.

c) fines and disgorgement, and

d) public censures.

However, in regard to criminal liability for legal entities there are caveats, as some industry commentators have noted.[160] The UK Government declined to "opt in" to Directive (EU) 2108/1673 (the sixth AMLD) on the following basis:

> "The UK's domestic legislation is already largely compliant with the Directive's measures, and in relation to the offences and sentences set out in the Directive, the UK already goes much further. Therefore, the Government decided not to opt in as we did not consider that opting in would enhance the UK approach to tackling money laundering."[161]

Although UK legislation does go further than the EU directives in many respects, that is not the case in regard to liability for legal entities; hence, we can assume, these inadequacies prompted the caveat "largely compliant" (as opposed to 'fully compliant'). As explained in FATF's UK 2018 MER, in regard to small companies, shell and front companies, the authorities tend to use the Insolvency Service to wind them up but the difficulty is imposing criminal sanctions on larger corporates. As noted in the 2018 UK MER:

> "Where legal persons are involved in offending, the UK will wind up shell or front companies and pursue prosecution of the natural persons or civil or regulatory actions. Complicit legal persons are investigated as part of the broader investigation, but rarely convicted. This is because the UK's ability to prosecute large legal persons for criminal ML offences under POCA and notable predicates such as fraud remains limited due to difficulties in proving criminal intent. Under the 'Identification Doctrine' established in UK case law, a criminal act can only be attributed to a legal person where the natural person committing the offence can be said to represent the "directing mind and will" of the legal person. In large companies with diffused decision-making responsibilities, proving this is extremely difficult, as was acknowledged by the NCA and the SFO. In response to this issue, the UK has made legislative changes to ease the intent requirements with respect to certain offences, including bribery and corruption and, with the enactment of the Criminal Finances Act 2017, tax evasion."

---

[160] "The EU's latest money laundering directive: does the UK comply?", Russell Hopkins and Olivia English, Bright Line Law, Lexology, 3 December 2018, https://www.lexology.com/library/detail.aspx?g=7d1db7a3-04b5-4d25-8e6a-f29eaec24cb2.

[161] "Eighth Annual Report to Parliament on the Application of Protocols 19 and 21 to the Treaty on European Union (TEU) and the Treaty on the Functioning of the Union (TFEU) in Relation to EU Justice and Home Affairs (JHA) Matters (1 December 2016 – 30 November 2017)", Home Office and Ministry of Justice, February 2018.

The MER also notes: "The ability to impose effective sanctions for legal persons could not be assessed due to a lack of ML convictions in this area."[162] We add that the presence of sanctions for some legal persons does not enable us to make ready judgments about their being 'effective' or otherwise. Neither special nor general deterrence of legal persons has been adequately researched scientifically, especially not in the context of large financial services firms. The Identification Doctrine gives rise to problems in fraud and corporate homicide as well as in money laundering cases.

3. Auxiliary Measures

The recoverable criminally derived benefit can be confiscated. Under POCA, if the court rules that the defendant has benefited from criminal conduct, the court can decide to make a confiscation order requiring the defendant to pay that amount. The UK has an *in personam* confiscation regime, and many confiscation orders are not paid or are paid only in part, despite the risk of extra prison sentences being imposed.[163] The regime is under review by the Law Commission in 2019-20.

4. Statistics

a. Number of Criminal Proceedings

The official statistics relating to crime and policing are maintained by the Home Office. Official statistics relating to sentencing, criminal court proceedings, et cetera are maintained by the Ministry of Justice. No data are available on the value of transactions involved in money laundering prosecutions, but there are 2,000 prosecutions annually for standalone money laundering or where money laundering is the principal offence.[164] As a point of comparison,

---

[162] We note that while the MER says in one place that legal persons are "rarely convicted", elsewhere the report states that there is a lack of money laundering convictions.

[163] "The gross value of confiscation order debt as at 31 March 2019 is £2,065million (2017-18: £1,961million) and has been impaired for accounting purposes to a net present value of £161million (2017-18: £152million), which is the estimate of the amount that is ultimately collectable." *HM Courts & Tribunals Service Trust Statement 2018-19*, p. 8. In other words, only 7.8% of the amount currently owing is collectible.

[164] FATF's 2018 MER states: "The UK routinely and aggressively identifies, pursues and prioritises ML investigations and prosecutions. It achieves around 7 900 investigations, 2 000 prosecutions and 1 400 convictions annually for standalone ML or where ML is the principal offence. The UK investigates and prosecutes a wide range of ML activity. Investigations of high-end ML (a long-standing risk area for the UK) have increased since being prioritised in 2014. These cases generally take years to progress to prosecution and conviction and limited statistics are available on high-end ML investigations, prosecutions and convictions prior to its prioritisation in 2014. As a result, it is not yet clear whether the level of prosecutions and convictions of high-end ML is fully consistent with the UK's threats, risk profile and national AML/CFT policies." The same report also notes: "Prosecution and conviction

there were only 65 prosecutions and 27 convictions of anyone for section 24 Drug Trafficking Offences Act 1986 money laundering offences between 1986 and the end of 1992, including probably only one non-conspiring banker.[165] In its annual reports, the UK's FIU provides some statistics on SARs that have resulted in seized cash and case studies.

A government reply to a detailed question about prosecutions and convictions led to the following answer:

Table 4. Number of prosecutions and convictions for offences under sections 327–330 POCA, 2013–2017

	2013	2014	2015	2016	2017
Prosecutions					
Section 327	981	880	1,063	841	878
Section 328	310	266	317	355	288
Section 329	1,050	944	921	797	737
Section 330	3	3	5	1	1
Convictions					
Section 327	520	447	550	601	537
Section 328	213	150	188	257	225
Section 329	527	541	594	567	581
Section 330	6	4	2	3	1

Note: The figures given in the pivot table relate to defendants for whom these offences were the principal offences for which they were dealt with. When a defendant has been found guilty of two or more offences it is the offence for which the heaviest penalty is imposed. Where the same disposal is imposed for two or more offences, the offence selected is the offence for which the statutory maximum penalty is the most severe.

figures are notably lower in Scotland. This may be due to Scotland's higher evidentiary threshold which can pose challenges in prosecuting criminal cases, particularly ML leading authorities to place a greater emphasis on general or catch-all offences."

[165] Michael Levi, "Incriminating disclosures: an evaluation of money-laundering regulation in England and Wales", *European Journal of Crime, Criminal Law, and Criminal Justice*, 3(2) (1995) 202–217.

Source: HC Deb, 24 October 2018, cW.

b. Number of Convictions

Evidence presented to the FATF stated that there are about 1,400 convictions annually.[166]

Table 5. Number of persons prosecuted and convicted for money laundering in the UK, 2013–2016

	2013	2014	2015	2016
	England and Wales			
Proceeded against	2,349	2,095	2,307	1,998
Convictions	1,269	1,143	1,336	1,435
	Scotland			
Proceeded against	13	42	18	21
Convictions	5	16	11	12
	Northern Ireland			
Proceeded against	156	135	133	125
Convictions	129	118	95	58
	TOTAL			
Proceeded against	2,518	2,272	2,458	2,144
Convictions	1,403	1,277	1,442	1,505

Source: FATF, *Mutual Evaluation Report – UK*, 2018.

There are substantial sums restrained and confiscated,[167] but these are not tracked back to SARs, nor did the UK Mutual Evaluation Report attempt to do so except via a few case studies.

Table 6. Assets restrained and confiscated 2014–2017

	2014/15		2015/16		2016/17	
	Number of orders	Amount (million)	Number of orders	Amount (million)	Number of orders	Amount (million GBP)
Total assets restrained	1,297	396.9	1 499	473	1,422	382.8
Total assets recovered		200.85		321.72		483.64
POCA confiscation	6,126	160.8	6,117	211.4	5,649	165.6

[166] FATF, *Mutual Evaluation Report – UK*, 2018, p. 59.
[167] Ibid, p. 74.

POCA civil and tax	24	6.55	15	11.33	13	8.52
POCA cash forfeiture	3,111	33.5	3,336	40.49	3,560	42.22
SFO disgorgement	0	0	1	6.2	1	258.2
FCA disgorgement	0	0	1	52.3	1	9.1

Source: FATF, *Mutual Evaluation Report – UK*, 2018.

Nor are confiscation data tracked routinely to types of offending, though some broad categories of data are revealed in the Mutual Evaluation Report.[168]

Table 7. Confiscation orders as a percentage of total value of offence types, 2014–2017

	2014/15	2015/16	2016/17
Total value of confiscation orders	**244.5**	**454.6**	**185.1**
Offence Type			
Money laundering	38.4	59.5	26.5
- as a percentage of total value	16%	13%	14%
Fraud	75.2	61.8	60.5
- as a percentage of total value	31%	14%	33%
Tax-related offending	61.1	259.7	18.6
- as a percentage of total value	25%	57%	10%
Drug offending	37.2	49.0	57.2
- as a percentage of total value	15%	11%	31%
Immigration crime	1.1	0.5	1.4
- as a percentage of total value	~0%	~0%	1%
Acquisitive crime	6.7	5.8	6.6
- as a percentage of total value	3%	1%	4%
Total (above offences)	**219.7**	**436.3**	**170.8**
- as a percentage of total value	**~90%**	**~96%**	**~92%**

Source: FATF, *Mutual Evaluation Report – UK*, 2018.

[168] Ibid, p. 83.

The most recent data for confiscation show that in 2019/20, just under £208m of the proceeds of crime were collected, within England, Wales and Northern Ireland: an 8% increase in money terms (but a fall in real terms) compared with 2014/15. [169]

• £139m was collected through confiscation orders, less than in the previous year.

• Just over £69m was collected through forfeitures in 2019/20. The current level of forfeiture represents the highest level seen in this time series, 2014/15 to 2019/20. This is partly due to the inclusion of bank account seizure and listed asset data for the first time.

• £208m, covering 812 bank and building society accounts, was frozen using Asset Freezing Orders: an unknown amount will eventually be confiscated.

• In 2019/20, 72% of Asset Recovery Incentivisation Scheme funds was invested in asset recovery work.

• In 2019/20, just over £31m was paid in compensation to victims from the proceeds of confiscation. The 2019/20 figure represents an overall increase of 29% since 2014/15.

A separate issue relates to so-called "high-end" money laundering, where initiatives were praised by the FATF but described by them as too early to show impact. The Solicitor General was asked in Parliament about the number of prosecutions and convictions, and replied:[170]

> "There is no legal definition or specific criminal offence of "high end" money laundering. The CPS does not maintain a central record of the number of defendants prosecuted for, and convicted of these offences. This information could only be obtained by examining CPS case files, which would incur disproportionate cost.
>
> CPS holds limited information on the number of offences which were charged and which reached a first hearing in the Magistrates Court. This does not equate to the number of defendants charged as single defendant may be charged with more than one offence.
>
> The figures for the period since 2014 are provided in the table below.

	2015–2016	2016–2017	2017–2018
Sections 327–330 POCA	4,542	4,866	4,813

[169] *Asset Recovery Statistical Bulletin 2014/15 – 2019/20 - England, Wales and Northern Ireland,* 2020, Home Office.
[170] HC Deb, 27 November 2018, cW.

> The SFO has prosecuted four individuals for money laundering offences since 2014. Two of these prosecutions resulted in a successful conviction in 2018. One of the two individuals unsuccessfully prosecuted was legally qualified."

(It is important to separate out those charged with laundering (i) the proceeds of crimes including fraud and corruption in which they were directly involved, and (ii) the proceeds of others' crimes: only some of the latter may be accurately described as professional money launderers.[171])

SANCTIONS FOR VIOLATIONS OF PREVENTIVE MEASURES

5. *Money Laundering by Violating Preventive Obligations*

As previously discussed, certain preventive measures are mandatory (e.g. KYC, due diligence). Typically, the responsibility rests with the MLRO and senior management. If they fail to implement an effective AML programme, including systems and controls in the regulated entity they work for, they can be held personally liable by criminal and regulatory authorities.

But in regard to the offence of failure to disclose, there are two schools of thought, with one arguing that an offence can be committed by negligence and the other arguing that negligence alone is not grounds for prosecution. According to this second school of thought, the state of mind required is that the offender must know or suspect or be reckless about whether the funds were proceeds of crime, and without some forensic evidence, such as a recorded phone call or email/file note, it may be difficult to prove beyond reasonable doubt.[172]

CDD, Reporting and Other AML-related Obligations

a. Special Criminal Laws against Individuals

See the previous section. Chapter 3 of Part 9 of the Money Laundering Regulations discusses the criminal penalties. A person is not guilty of an offence if that person has taken all reasonable steps and conducted all due diligence to avoid committing an offence.

---

[171] See Michael Levi and Melvin Soudijn. 2020. 'Understanding the Laundering of Organized Crime Money', *Crime and Justice*. It is also important to distinguish between professional money launderers and launderers who have professionally qualifications, though the categories may sometimes overlap.

[172] In the law of England and Wales, recklessness may be defined as the conscious taking of an unjustified risk. Negligence is unreasonable conduct that creates risk, while gross negligence is a high degree of negligence that may deserve criminal punishment. In *R v G & R* [2003] UKHL 50, it was determined that recklessness was punishable criminally where: (i) a circumstance when he is aware of a risk that it exists or will exist; (ii) a result when he is aware of a risk that it will occur; and it is, in the circumstances known to him, unreasonable to take the risk."

Additionally, failure to make a disclosure on the PSC register and failure to comply with notices requiring someone to provide information are criminal offences.

The information is entered into the central Companies Registry based on documents provided by the company. The information entered is checked against the original documents. However, the central companies registry is not responsible for investigating and confirming that the individuals identified as owners in the company's documentation are indeed its true owners.

According to regulation 88 of the Money Laundering Regulations, a person commits an offence if, in purported compliance with the Regulations, this person provides information to any person which is false or misleading and:

> "(a) that person knows that the information is false or misleading; or
> (b) that person is reckless as to whether the information is false or misleading."

A person guilty of an offence under the above paragraph is liable:

> "(a) on summary conviction—
> (i) in England and Wales, to imprisonment for a term not exceeding three months, to a fine or to both,
> (ii) in Scotland or Northern Ireland, to imprisonment for a term not exceeding three months, to a fine not exceeding the statutory maximum or to both;
> (b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

The above applies to the obliged entities in the context of the requirement to comply with the Money Laundering Regulations. It includes false statements made by the first line of defence of an obliged entity to the second line of defence of the same obliged entity or a by an obliged entity to the authorities or to other obliged entities.

Regulation 86 states that in deciding whether a person has committed an offence the court must decide whether that person followed guidelines issued by the European Supervisory Authorities in accordance with the EU Money Laundering Directive, the UK Money Laundering Regulations or guidance issued by the FCA or another body and approved by the UK Treasury. A person is not guilty if that person took all reasonable steps and exercised all due diligence to avoid committing the offence.

Regulation 87 relates to persons in the regulated sector knowingly prejudicing an investigation into a violation of the regulations.

According to regulation 90, even if the offence was committed outside of the UK by a person in the UK, it will be treated, for the purposes of legal proceedings, as if it has been committed within the UK

Additionally, according to the Companies Act, criminal sanctions may be imposed on companies and their officers for not complying with their beneficial ownership information obligations.

b. Administrative Sanctions against Individuals

Administrative sanctions include suspension or cancellation of authorised status or prohibition imposed on managers. If solicitors allow their client accounts to be used for banking activities by clients that are not related to the provision of particular legal services, or fail to take due diligence measures required, they can be sanctioned by the Solicitors Disciplinary Tribunal following action that is normally taken by the SRA or by the Law Society's regular inspection of records.

c. Sanctions against Legal Entities

The range of sanctions are as above. The various supervisory bodies can initiate the sanctions (e.g. the FCA, HMRC). More specifically, in regard to civil penalties, according to Part 9 of Chapter 2 of the Money Laundering Regulations, sanctions may include financial penalties, a censuring statement, cancellation or suspension of regulatory permissions, payment services provider registration or authorisation, or other restrictions, as well as prohibitions on management.

6. Statistics

a. Number of Investigations and Sanctions

The UK's FIU annual report provides statistics on how many SARs have been filed, how many have been passed onto other bodies, intelligence disseminated to foreign agencies, and:

- restraint sums;
- cash seizure sums;
- funds indemnified by HMRC;
- funds recovered by HMRC;
- some cases with arrests recorded.

There is no consistent and regular publication of statistics, and no collated list of sanctions against regulated or other persons for violations of prevention measures, though the FATF Mutual Evaluation Report stimulated regulators to produce data, which may continue hereafter.

In the period 2012–2018, the FCA concluded 14 AML/counter-terrorist financing enforcement cases relating to 10 firms and four individuals. HMRC undertook a modest number of cases against breaches of the Money Laundering Regulations: in the period June 2017–2018, four firms were issued with penalties (all under £6,000) for breaches; two firms were fined a total of £466.50 (but names were not published because the acts were minor); while in the period 2007–2017 (when the Regulations were revised), 535 firms were fined a total of £2.4 million.[173] A total of 101 individuals were convicted of money laundering in the period April 2010–April 2018 as a result of HMRC investigations. The average size of fine for HMRC breaches went up from £1,310 in 2016/17 to £3,450 in 2017/18. In 2018-19, HMRC imposed 131 fines totalling £1,173,022, compared with 655 fines totalling £2,258,656 the previous year. It prosecuted 2 people for money laundering regulation breaches, compared to one the previous year.

The UK Mutual Evaluation Report provides limited information on sanctions by the FCA, set out below:[174]

Table 8. Penalties for money laundering imposed by the Financial Conduct Authority, 2012–2017

	2012/13	2013/14	2014/15	2015/16	2016/17	Total
Fines	5	4	1	1	3	14
Section 166 FSMA	11	14	6	6	5	42
Attestations	15 between June 2013 and June 2016					15
Business restrictions	12 between 2012–14			2	6	20
Early Interventions		4	8	8	7	27

Source: FATF, *Mutual Evaluation Report – UK*, 2018.

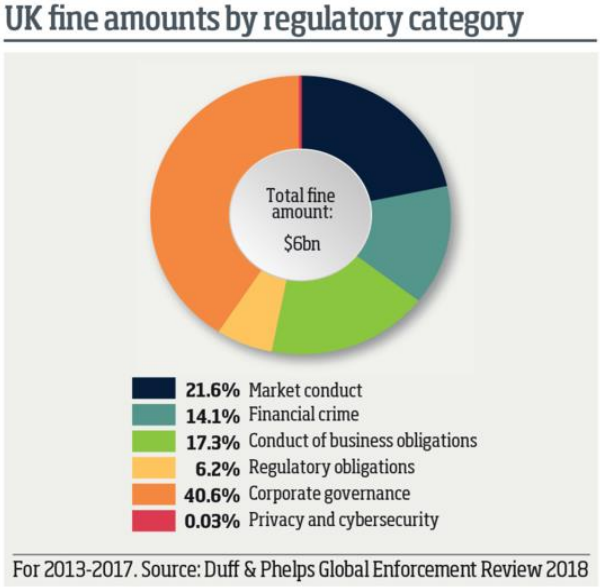
Section 166 FSMA refers to the appointment of skilled persons (e.g. senior money laundering experts from the private sector) to monitor the firm's AML activities and to suggest enhancements, for which monitoring the firm has to pay.

Another way of looking at the data in the context of the other responsibilities of the FCA is provided by Duff and Phelps:

[173] https://www.gov.uk/government/publications/businesses-not-complying-with-money-laundering-regulations-in-2018-to-2019/current-list-of-businesses-that-have-not-complied-with-the-2017-money-laundering-regulations. See https://www.gov.uk/guidance/money-laundering-regulations-appeals-and-penalties for the procedures.

[174] FATF, *Mutual Evaluation Report – UK*, 2018, p. 134.

Figure 2. UK fine amounts by regulatory category, 2013–2017



Source: Duff and Phelps, Global Enforcement Review 2018.

Subsequently, consulting firm Encompass has reviewed regulatory penalties imposed for AML violations in calendar year 2019 around the world, and (including regulators such as the Gambling Commission as well as the FCA), the UK was second to the US globally, with 12 fines totalling $388.4m.[175] **The imposition of regulatory penalties should be viewed as an activity measure, not necessarily an effectiveness measure, though the total or almost total absence of penalties may be a sign of merely formal or symbolic compliance.**

The Law Society's Solicitors' Disciplinary Tribunal publishes its decisions, but in the case of money laundering or predicate crimes, such sanctions would normally occur post-conviction, and "money laundering" is not available as a search term on its case database.[176] The SRA also publishes a selection of cases, but these give little insight into their relationship to money laundering and are intended to enable the public to check whether a particular solicitor has been subject to sanctions or not.[177] The SRA usually prosecute via the Solicitors' Disciplinary Tribunal because the latter has the power to strike off lawyers. The SRA also conducted a thematic review

[175] https://www.encompasscorporation.com/blog/encompass-aml-penalty-analysis-2019/

[176] See http://www.solicitorstribunal.org.uk/judgment-search-results#judgment-list

[177] See https://www.sra.org.uk/consumers/solicitor-check/recent-decisions/ for recent decisions; and https://www.sra.org.uk/consumers/solicitor-check.page for individual lawyers' checks.

of law firms.[178] In that review of 50 firms, designed to test the sector's compliance with new, tougher AML regulations, the SRA found only a third had carried out a mandatory risk assessment of their AML procedures or were in the process of implementing one. In six of the 50, which ranged from high street to City firms, the SRA found serious concerns that merited "ongoing disciplinary processes".

In 2015–18, the SRA closed down eight law firms over money laundering concerns, although in some cases the action was preventive and took place without definitive proof of their wrongdoing. A further 14 companies shut down of their own accord after it raised concerns. The SRA has also referred 49 lawyers to the solicitors' disciplinary tribunal.

HMRC is not a membership organisation; the application to register for money laundering supervision from a prospective regulated firm is often the first AML/CTF contact HMRC has with the applicant and the first opportunity to refuse the right to practice. In 2018-19, 13,136 businesses applied to be registered with HMRC for AML supervision. 1,082 were refused under regulation 59 and 628 registrations were cancelled or suspended, under regulation 60. HMRC also conducts fitness and propriety tests on certain individuals in MSBs and TCSPs. Under the MLRs 2017, in addition to the 'fit and proper' tests in MSBs and TCSPs, HMRC is also required to conduct criminality tests for key individuals in accountancy service providers, high value dealers and estate agency businesses, ensuring that individuals who have a relevant criminal conviction are not able to hold relevant positions, including being a beneficial owner, officer or manager of a firm or sole practice (known as BOOMs). In 2019-2020, HMRC received 21,760 applications for individuals to become BOOMs, of whom 6% were rejected, either by being part of a rejected company application or for individually failing their fitness and propriety test. In 2017–18, HMRC imposed 655 penalties against accountants, estate agents and dealers in luxury goods such as art and jewellery, down from 901 in 2016–17. This may have reflected a greater focus on more complex cases.

The UK Gambling Commission's principal role is to protect customers from misconduct by gambling firms and to protect "vulnerable" gamblers from being encouraged to gamble. The Gambling Commission is the supervisory authority for approximately 208 casinos; 163 of these are online casinos, 36 are land-based and 9 have a license allowing them to do both. Any gambling company operating in the UK, or with customers based in the UK must hold the appropriate

[178] https://www.sra.org.uk/sra/how-we-work/reports/preventing-money-laundering-financing-terrorism.page.

license issued by the Gambling Commission. Within these licensed businesses, individuals who hold certain key management functions must hold personal management licenses. There are an equivalent of 4 employees dedicated to AML/CTF supervision in the Gambling Commission. However, AML/CTF is integrated into the Commission' wider work (legal, intelligence, licensing, compliance and enforcement) which also assist with AML/CTF supervision. Across these areas, there are an equivalent of 150 employees.

The Gambling Commission's risk assessment classifies all casinos as high risk: there are 88 higher-risk casinos, including 19 land-based, 62 online and 7 whose licenses allow them to do both. The Gambling Commission separates those casinos with higher impact and higher likelihood of risk based on many risk indicators, such as: the businesses' gross gambling yield, consumer impact, jurisdictional risk, exposure to Politically Exposed Persons, higher risk products, channels or means of payment. The Commission considers land-based casinos to have a higher level of risk than other gambling sectors, due to a combination of compliance failures and the high level of cash transactions. However, online casinos face additional risks such as customers not being physically present for verification purposes and increased accessibility.

It has also imposed some penalties, though only one for money laundering breaches alone: the AML actions relate to failure to pursue checks on the source of funds that were later discovered to be stolen. One fairly recent case – a £7.1 million fine on Daub Alderney – was part of an announced crackdown by the Commission in 2018 and was for failure to conduct a money laundering risk assessment on their customers as required under the conditions of licence, as well as under money laundering legislation.[179] Another recent case – a £6.2 million penalty on William Hill bookmakers – is set out in the following footnote.[180] Another £2.2 million penalty was

[179] Gambling Commission, "Daub Alderney to pay £7.1m fine for anti-money laundering and social responsibility failures", 13 November 2018, https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/Daub-Alderney-to-pay-7.1m-fine-for-anti-money-laundering-and-social-responsibility-failures.aspx.

[180] Gambling Commission, "William Hill to pay £6.2m penalty package for systemic social responsibility and money laundering failures", 20 February 2018, https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/William-Hill-to-pay-6.2m-penalty-package.aspx.
"A Gambling Commission investigation revealed that between November 2014 and August 2016 the gambling business breached anti-money laundering and social responsibility regulations. Senior management failed to mitigate risks and have sufficient numbers of staff to ensure their anti-money laundering and social responsibility processes were effective. This resulted in ten customers being allowed to deposit large sums of money linked to criminal offences which resulted in gains for WHG of around £1.2m. WHG did not adequately seek information about the source of their funds or establish whether they were problem gamblers.

imposed on Paddy Power,[181] a £2.3 million penalty on Gala Interactive,[182] and a £80,000 penalty on Stan James Online.[183] In May 2019, The Gambling Commission imposed £4.5 million in "penalty packages" on online casinos,[184] and this was followed by further penalties, the largest of which was a £5.9 million fine on Ladbrokes for "past failures".[185] Other sanctions are published, but none visibly relates to money laundering failures.[186] In none of them is it clear that the firms were actively assisting people to launder money in the sense of concealing the source of funds in order to hide the audit trail: the gambling firms were increasing their turnover and profits by failing to carry out their licence responsibilities or failing to think through the control process. Nor is it clear that any of the gamblers were gambling as a placement or layering exercise: it appears that they were simply obsessed with gambling. So it is plain that as with the SRA, the Gambling Commission conducted a "blitz" on its regulatees as part of an attempt to get them to take their AML responsibilities more seriously.

WHG will pay more than £5m for breaching regulations and divest themselves of the £1.2m they earned from transactions with the ten customers. Where victims of the ten customers are identified, they will be reimbursed. If further incidents of failures relating to this case emerge, WHG will divest any money made from these transactions.
WHG will also appoint external auditors to review the effectiveness and implementation of its anti-money laundering and social responsibility policies and procedures and share learning with the wider industry …

[181] Gambling Commission, "Paddy Power Betfair to pay penalty package for social responsibility and money laundering failures on its gambling exchange", 16 October 2018, https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2018/Paddy-Power-Betfair-to-pay-penalty-package-for-social-responsibility-and-money-laundering-failures-on-its-gambling-exchange.aspx.

[182] Gambling Commission, "Gala Interactive to pay £2.3m penalty package following social responsibility failures", 6 November 2017, https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Gala-Interactive-to-pay-2.3m-penalty-package.aspx.

[183] Gambling Commission, "Stan James Online to pay £80,000 penalty package for social responsibility and money laundering failures", 30 October 2017, https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/2017/Stan-James-Online-to-pay-80000-penalty-package.aspx.

[184] "InTouch Games Limited will pay £2.2m, Betit Operations Limited will pay £1.4m, and MT Secure Trade will pay £700,000 in lieu of financial penalties, and BestBet will pay a financial penalty of £230,972. The penalty packages relate to the businesses failings to put in place effective safeguards to prevent money laundering and keep consumers safe from gambling harm. The penalty packages form part of an ongoing investigation into the online casino sector. Over the last 18 months the regulator has conducted assessments of, or engaged with, 123 online operators – and of the 45 told to submit an action plan to raise standards 38 have already showed signs of improvement. A further 34 were compliant with standards expected by the Commission or had minor issues which have been, or are in the process of being, remedied. Since the investigation began five operators have surrendered their licence and can no longer transact with consumers in Britain. In November 2018 three companies paid nearly £14m in penalty packages as result of their failings to put in place effective safeguards to prevent money laundering and keep consumers safe from gambling-related harm." https://www.gamblingcommission.gov.uk/news-action-and-statistics/News/widespread-regulator-action-results-in-further-45m-in-penalty-packages-for-online-gambling-sector.

[185] https://www.gamblingcommission.gov.uk/news-action-and-statistics/news/news.aspx?searchKeywords=&categories=0/1/24/41&page=0.

[186] Gambling Commission, "Operator licences – regulatory decisions", https://www.gamblingcommission.gov.uk/PDF/Regulatory-sanctions-register-operators.pdf

Following supervisory activity, the Commission took informal action against approximately 32% of firms subject to a DBR and 15% of firms subject to a visit. Formal actions were taken following approximately 18% of the DBRs and approximately 11% of visits. Other supervisory tools used by the commission include: proactively maintaining oversight of the largest operators by conducting regular assessments of their policies and procedures, thematic pieces of work on specific topics, as well as requiring the largest operators to produce an annual assurance statement signed off at board level. This encourages licensees to reflect on processes, including AML and CTF, from board level down and ensure they have worked to raise standards in identifying, reviewing, and correcting compliance issues. In 2018-19, out of 13 cases for AML failings, seven related to individuals holding management licences within their respective gambling business and six related to firms. These failings resulted in:

- 11 entities receiving warnings
- 3 having additional conditions imposed on their license to operate
- 1 licence being revoked
- 5 financial penalties, amounting to £17 million in total (up from £6.4 million in one case the previous year).

HM Treasury produces a consolidated annual report on the supervision and sanctions imposed by the AML/counter-terrorist financing supervisory bodies under its jurisdiction, with reports that have expanded their scope recently. It reveals that in 2018-19, 12 out of the 22 legal and accountancy PBSs collectively issued 237 fines, amounting to £499,051 in total. The average amount fined varied significantly between PBSs (between £192- £48,571) but approximated to £2,105 overall. This is a significant increase in enforcement action by PBSs compared to the previous financial year when 11 PBSs issued a total of 135 fines amounting to £211,450. However although there may be informal and occupational sanctions in addition to any formal penalties, one might question the seriousness of these penalties in both general and specific deterrence, even if they arguably mark the gravity of the offences (whose harmfulness is not set out). The most recent report reveals the following (with data from the previous year in brackets, where available):

Table 9. Enforcement action by members of the Accountancy Affinity Group 2018-2019

2018-19	Memberships cancelled	Memberships suspended	Number of Fines	Total amount of Fines
Association of Chartered Certified Accountants	0 (9)	0 (1)	0 (0)	0 (£0)
Association of International Accountants	4 (1)	2 (0)	9 (2)	£1,800 (£400)
Chartered Institute of Management Accountants	2 (1)	0 (0)	0 (1)	£0 (£675)
Chartered Institute of Taxation	0 (0)	0 (0)	72 (28)	£15,244 (£3,378)
Association of Taxation Technicians	0 (0)	0 (0)	53 (12)	£10,200 (£2,394)
Institute of Chartered Accountants of England & Wales	8 (8)	0 (0)	22 (11)	£55,907 (£77,625)
Institute of Chartered Accountants of Ireland	0 (0)	0 (0)	6 (2)	£1,500 (£750)
Institute of Chartered Accountants of Scotland	0 (0)	0 (0)	1 (0)	£5,000 (£0)

Institute of Certified Bookkeepers	0 (0)	0 (0)	18 (16)	£7,352 (£4,115)
Institute of Financial Accountants	0 (2)	0 (0)	1 (1)	£750 (£500)
Association of Accounting Technicians	2 (4)	0 (0)	43 (53)	£48,046 (£47,112.96)
International Association of Bookkeepers	0 (1)	0 (0)	0 (0)	0 (£0)

Table 10. Enforcement activity by members of the Legal Sector Affinity Group

2018-19	Memberships cancelled	Memberships suspended	Number of Fines	Total amount of Fines
Solicitors Regulation Authority	7 (1)	1 (1)	7 (7)	£340,002 (£70,500)
Law Society of N. Ireland	0 (0)	0 (0)	0 (0)	0 (0)
Law Society of Scotland	2 (1)	0 (0)	4 (2)	£11,500 (£4,000)
Council of Licenced Conveyancers	0 (1)	0 (0)	0 (0)	0 (0)
Bar Standards Board	0 (0)	0 (0)	0 (0)	0 (0)
General Councilof the Bar of N. Ireland	0 (0)	0 (0)	0 (0)	0 (0)

Chartered Institute of Legal Executives Regulation	0 (0)	0 (0)	0 (0)	0 (0)
Faculty of Advocates	0 (0)	0 (0)	0 (0)	0 (0)
Faculty Office of the Archbishop of Canterbury	0 (1)	0 (0)	0 (0)	0 (0)

Source: HM Treasury, *Anti-money laundering and counter- terrorist financing: supervision report 2018-2019.*

b. Number of Convictions

There is no one single source that would consistently publish this data. The most likely agency to prosecute for regulatory failures is the FCA, and penalties imposed by the FCA 2012–2018 totalled £343,346,924 on firms and £92,700 on individual MLROs. However, these include regulatory penalties, and criminal prosecutions are not separated out. Moreover, totals can be distorted by the effect of individual cases or connected cases that are unlikely to recur. The collateral financial consequences for individual MLROs are not included but may be considerable.

The 49 lawyers referred to the Solicitors' Disciplinary Tribunal resulted in 12 being struck off, the suspension of 13 and more than £800,000 in fines. In April 2017, the international firm Clyde & Co was ordered to pay a fine of £50,000 and three of its lawyers were fined £10,000 each over various allegations, including failure to comply with accounting rules and to act in accordance with money laundering regulations. The three partners allowed a client account to be used as a banking facility in breach of accounting rules and the code of conduct, a failure to act in accordance with their obligations under the Money Laundering Regulations 2007.[187]

HMRC fined companies £2.3 million in 2017–18, up from £1.2 million a year earlier. This constituted £3,500 per penalty, and unless the businesses were very unprofitable, this looks like

[187] Max Walters "Clyde & Co faces £50,000 fine after SDT ruling", Law Society Gazette, 4 April 2017, https://www.lawgazette.co.uk/law/clyde-and-co-faces-50000-fine-after-sdt-ruling-/5060549.article.

a modest sanction.[188] In 2018–2019, HMRC recovered more than £41 million using the confiscation, civil recovery and cash forfeiture regimes in POCA and successfully prosecuted 32 individuals for money laundering offences and failing to follow regulations. West London money transmitter Touma Foreign Exchange Ltd received a £7.8 million penalty for a wide range of serious failures under the Money Laundering Regulations. Between June 2017 and September 2018, the business breached rules on risk assessments and associated record keeping; policies, controls and procedures; CDD measures; and adequate staff training.[189] This included a failure to submit its MLRO for vetting by HMRC.

THE MIXTURE OF MONEY LAUNDERING AND OTHER AML-RELATED SANCTIONS

There is no prohibition on combining sanctions for money laundering with sanctions for the violation of preventive obligations, but in a UK context this would be regarded as a highly theoretical question. Someone could be subject to professional disciplinary sanctions on the same set of facts as a criminal prosecution – whether successful or not – and, if the evidence was different, to support parallel charges, this would not offend any *ne bis in idem* principle, in the same way that alternative charges of differential seriousness for violence, sex and motoring offences could be indicted. This might be the basis for plea bargaining, or the court or disciplinary body might produce a different verdict on the parallel charges.

---

[188] In *N Bevan Limited v HMRC* [2016] TC 05404 the First Tier Tribunal (FTT) upheld a HMRC penalty imposed on a small one-person accountancy firm not supervised by any professional body for not keeping up with their AML obligations. Following two site visits and a warning letter, HMRC imposed a penalty on the taxpayer for failure to comply with its requirements in respect of customer due diligence, ongoing monitoring of clients, record keeping, and risk assessment. The taxpayer argued he had not breached any requirements. Although he could not produce client or other records to show procedures undertaken, he only acted for clients known for many years, only taking on new clients where they were connected to existing clients, and he used HMRC's authorised agent facilities to confirm the information provided to him by clients and as an electronic record of the information he gathered.
The Tribunal in reaching its decision considered the guidance issued by the Consultative Committee of Accountancy Bodies (CCAB) in August 2008, noting that if a taxpayer had complied with this guidance, it would not have breached the regulations. It upheld the penalty, finding that: the taxpayer had failed to establish proper verification, monitoring and record keeping processes despite a clear warning to do so; the only evidence provided that these were in place was the taxpayer's assertion; and using HMRC's online tax agent system to record information on clients does not comply with money laundering requirements.
The FTT did however change the level of the penalty: it was limited to 10% of the firm's gross revenue, and the mitigation factor was reduced from 50% to 20%: HMRC had been "over generous" as the taxpayer had been given the opportunity to address their concerns but did nothing.

[189] HMRC Press Release, "Money sender fined record £7.8 million in money laundering crackdown", 4 September 2019, https://www.gov.uk/government/news/money-sender-fined-record-78-million-in-money-laundering-crackdown.

VIII. THE USE OF CASH AS A MEANS OF PAYMENT

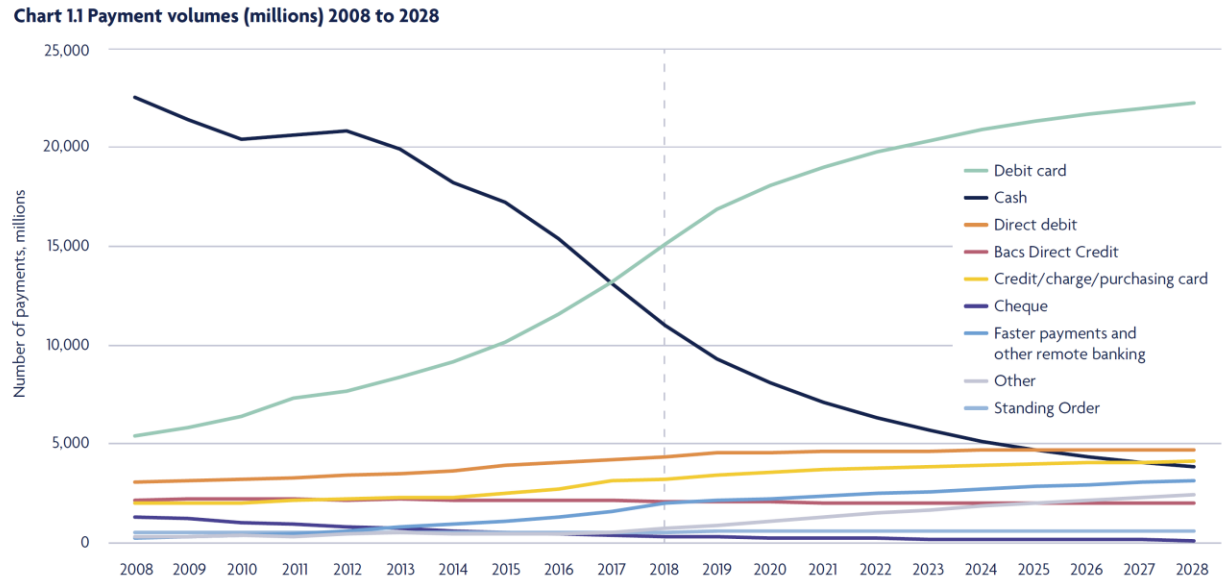
There are no legislative limits on the use of cash as a means of payment in the UK, though there are requirements on the reporting of large cash payments in line with EU requirements. In the UK, cash dropped from 60% of all payments in 2008 to 28% in 2018, and falling during Covid-19. Almost one in seven of the population, and one in four of those aged 16 to 34, chose to live a largely cashless life in 2019: defined as either not using notes and coins at all, or only once a month. In 2018 the figure was one in 10 of the population, or 5.4 million people. In 2017 it was 3.4 million.

In 2017, debit card payments overtook cash as the most popular form of payment in the UK.[190] Consumers used their debit cards 15.1 billion times in 2018, up 14% each year compared to 2016. The number of cash transactions fell by 31% to 11 billion transactions in the same period, though it remained the second most frequent means of payment, with 1.9 million people who almost always used cash. Use of contactless payment cards has been rising very rapidly to 7.4 billion transactions. Over two thirds (69%) of people in the UK used contactless payments even before the Covid-19 pandemic began.

By the end of 2018 there were nearly 124 million contactless cards in circulation, with 84% of debit cards and 64% of credit cards in Britain having contactless functionality. UK Payments has provided the chart below, containing historical and predicted data.

[190] https://www.ukfinance.org.uk/wp-content/uploads/2018/06/Summary-UK-Payment-Markets-2018.pdf; UK Finance, *UK Payment Markets Summary 2019*, June 2019, https://www.ukfinance.org.uk/sites/default/files/uploads/pdf/UK-Finance-UK-Payment-Markets-Report-2019-SUMMARY.pdf.

Figure 3. Payment volumes (millions), 2008–2028



Source: UK Finance, *UK Payment Markets Summary 2019*, June 2019.

IX. RECENT CHANGES IN THE UK

A number of changes are significant, in addition to those discussed earlier.

NATIONAL ECONOMIC CRIME CENTRE

The NECC – located within the National Crime Agency - is partly a governmental response to the patchwork of national and local policing and non-police agencies involved in loosely defined 'economic crime'. The 2017 Anti-Corruption strategy developed by the Cameron government identifies six key priorities, among which was the strengthening of the UK's integrity as a global economic centre. It planned to achieve this through, *inter alia*, an increased "strategic oversight from across the government that enables... agencies to prioritise activity better, drives performance and aligns funding and capability" as well as through "stronger law enforcement, prosecutorial and criminal justice action".[191] The later Serious and Organised Crime Strategy 2018 confirmed the NECC as the national authority for the UK's operational response to economic crime.[192] There is as yet (reasonably) no evaluation of its impact, but it

[191] https://www.gov.uk/government/publications/uk-anti-corruption-strategy-2017-to-2022
[192] https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2018

aims to energise both fraud and 'illicit finance' enforcement efforts via both pursuit of offenders and better prevention and resilience, in accordance with the 'Four Ps' imported into the SOC from counter-terrorism strategy. In 2019, the DG of the NCA issued a very rare power to task police forces to work with the NECC to set up a dedicated project, OTELLO, to deliver an improved response to 'vulnerable victims' of fraud across law enforcement. The NCA states that in 2019-20:

> "The NECC has made a strong start in providing system leadership in tackling the fraud threat, working close with law enforcement partners. During the year, as a direct result of JMLIT support: 56 arrests were made; 3,740 bank customers had their accounts closed; £3,398,776 in funds were restrained or seized. NCA activities have led to £9m worth of cash forfeitures and an additional £9m worth of cash seizures. Intelligence gathered by the Agency has supported the seizure of a further £17.6m by other agencies."[193]

Praiseworthy though that is, it (and asset freezing or forfeiture generally) is a tiny proportion of the amount of money obtained by serious offenders in the UK, let alone the UK's role as a laundering conduit for proceeds of crime elsewhere.[194] The NECC is also responsible for the Foreign Bribery Clearing House, a central co-ordination and de-confliction service for bribery investigations with a UK connection. JMLIT supported 18 requests relating to foreign bribery investigations in 2019-20. It is early days to judge the difference it has made, but there is a need to co-ordinate and allocate work between the police, NCA, and Serious Fraud Office, as well as to promote prevention. However, this has to be done mainly by persuasion, and there are very few investigative resources around the UK and its separate nations to upscale the Pursue function, even if the proposed Economic Crime Levy on regulated persons substantially enhances the SARs infrastructure. The structural problem remains the same as that observed in my commentary on the Fraud Commission concept advocated by Lord Roskill's Fraud Trials Committee in 1986: the absence of a power to increase net resources.[195] So clarity, prioritisation and persuasion are valuable skills possessed by the NECC leadership, but there are clear limits to what it is capable of achieving, absent a shift of resources from other areas to economic crime

[193] *National Crime Agency Annual Report and Accounts 2019-20*, p.22

[194] By way of comparison, the Economic Crime Plan states (para 1.3): "The Home Office estimates that the social and economic cost of fraud to individuals in England and Wales is £4.7 billion per year and the social and economic cost of organised fraud against businesses and the public sector in the UK is £5.9 billion. In 2018, UK Finance estimates that £1.2 billion was stolen by criminals committing authorised and unauthorised fraud, with the banking sector estimated to have prevented a further £1.7 billion in unauthorised fraud." To this should be added the billions from other forms of organised crime.

[195] Michael Levi, 'The Roskill Fraud Commission revisited: An assessment', *Journal of Financial Crime*, 2003, 11(1), pp. 38-44

(and police skills enhancement for this shift) or new expenditure in the now postponed Comprehensive Spending Review.

The other major arena for potential change is the first government Economic Crime Plan (2019-2022), which was launched in July 2019 and sets out the UK government's response to a range of economic crimes impacting the UK, including money-laundering, fraud, market abuse and bribery. It sets out a public-private response to these problems, containing 52 actions under seven priorities areas with deadlines for achieving these actions. The UK Government has been engaged in efforts to measure the components of economic crime better and to develop controls via the Joint Fraud Task Force as well as JMLIT, with a controversial Economic Crime Levy on regulated firms to raise funds for improvements in the fast-decaying ELMER technology, and – much disputed, since there are very diverse interests among AML-regulated firms – to improve fraud controls. The areas in which most progress has been made include UK Finance efforts to clarify the responsibility for payment card fraud costs and to take a greater share of that for the banks, reduce automated push payment frauds, and bring about other techniques to reduce the risk of misrepresentation of identity when transferring funds. The UK has good counter-fraud data sharing. However, other types of fraud have raised bigger difficulties, and the Financial Conduct Authority has received serious criticism for its inability/unwillingness to intervene quickly enough in cases of pension liberation fraud, and a range of consumer investment scams that have become more common as legitimate returns on savings have fallen.

The Serious Fraud Office self-selects its cases, but though it has negotiated large transnational bribery settlements, some major fraud cases involving senior executives and major corporations have been unsuccessful, for reasons that are disputed, with claims by defence lawyers of lack of competence and high staff turnover, and complaints by the SFO (and by the Crown Prosecution Service fraud lawyers) of over-burdensome disclosure requirements and an inability to offer sufficient incentives for guilty pleas, US-style. Jury trial remains a contentious issue, but problems in prosecuting major frauds have been long-running, going back to before the formation of the SFO in 1987.[196]

A recent inspection report concluded that[197]:

> "The SFO has clear and well documented internal casework processes, contained in an operational handbook which sets out what is expected and in some instances mandated.

[196] Michael Levi, *The Investigation, Prosecution, and Trial of Serious Fraud*, Royal Commission on Criminal Justice Research Study No.14, 1993, London: HMSO.

[197] https://www.justiceinspectorates.gov.uk/hmcpsi/inspections/case-progression-sfo-oct-19/

However, the inspection found that there is inconsistency in application, with individual case managers operating in their preferred way and this can impact the effectiveness and efficiency of case progression. In some of the cases examined inspectors found that this inconsistent and personal approach can hamper the ability of staff joining a team to get to grips with the case, and of those working on more than one team at once to understand what is expected of them. Whilst there is a clear internal guidance and expectations the SFO could do more to improve its assurance processes to ensure full and appropriate compliance. The SFO have recently commissioned a new case management system which they hope will address some of the concerns identified.

Unused material was handled reasonably well, and there were examples of very good consideration of the material and strong disclosure strategies. However, there were inconsistencies in practice here, too. Compliance with the handbook and the methods of different case controllers in several of the cases we examined resulted in inconsistencies in approach and hampered case progression, particularly when a peer review highlighted problems, or a new case controller changed the original case strategy. In these instances this caused delay and re-work.

Cases are accepted for investigation in a timely manner, but delays then occur. This is often as a result of two key blockages: firstly, the allocation of a case controller and a suitable team takes too long in some cases; and secondly, the digital forensic unit is significantly behind in its processing of the digital material the case teams need to investigate. Resourcing inevitably plays a part in this. The SFO has carried out significant work to address the concerns with regard to processing the backlog of digital material but suffers from the same issues that face many in the criminal justice system with the increases in digital material. Whilst there is a strategic and tactical co-ordination group, in its current form it does not examine cross-team resourcing as the case has yet to be allocated to case teams when discussion takes place. The SFO needs to develop a strategic approach to resourcing and case management.

There are opportunities for learning and development, and staff report that they receive the training they need to do their jobs. The SFO has trained and supported staff to become investigators and accountants, both disciplines where there are shortages, and this is part of a high-level strategy to support more effective case progression by having the right balance of staff to be able to support casework. However given some of the issues set out in this report the SFO should consider developing specific case

progression training or increasing the focus on case progression current training packages.

There are various strands to the oversight and assurance of casework, including case review panels, Heads of Divisions' meetings with case teams, peer reviews and performance data. Many of the opportunities for assurance tend not to have a specific focus on case progression and look at the entirety of the case. We found that case review panels varied in frequency and depth of analysis, and tend to be more focussed on legal issues than case progression. We set out that Heads of Division could do more to challenge, influence and quality assure cases that are not progressing effectively.

Senior managers are fully engaged with partners and stakeholders, and there are agreements and protocols in place and an international team in the SFO; we saw that this could have tangible benefits for mutual assistance and case progression. There was one very good example of how this stakeholder engagement aided case progression in our file examination.

The SFO has made a greater commitment to victims and witnesses; there are more resources applied, and clearer expectations set, which have led to improved communications with victims and witnesses. The requirement for case managers to develop a victim and witness strategy at an early stage is leading to more timely determination of a person's status as a suspect, victim or witness, which is improving the quality of investigative decisions. Inspectors noted major improvements since the last inspection in 2016.

Inspectors identified two examples of good practice, and made seven recommendations. The recommendations were:

1. The Serious Fraud Office should develop a resourcing model that takes into account staff skills and time available to progress cases effectively.
2. The Serious Fraud Office should review resourcing in a holistic manner to ensure equity across cases in allocation of the teams and skills and reconsider allocation of the case controller and team when it becomes apparent that cases are not being taken forward promptly after acceptance.

3. The Serious Fraud Office should review resourcing across divisions to ensure that resources are allocated according to case needs, and in such a way that when changes are required, there is as little disruption as possible to case progression.

4. The Serious Fraud Office should be clear about the use of independent counsel, including guidance for case controllers on their deployment and monitoring, and a mechanism for evaluating the value for money they provide.

5. The Serious Fraud Office should develop understanding across the casework divisions of the impact of seizures on the digital forensic unit, and the need to be proportionate in their demands and expectations of this unit. This should be accompanied by measures to significantly reduce the impact of current delays on case progression.

6. The Serious Fraud Office should consider how it can improve the focus and delivery of training to support case progression. The Serious Fraud Office needs to develop a programme of learning and development that delivers the core skills for effective case progression.

7. Heads of Division should set and monitor key milestones in the investigation and prosecution of cases, and should enforce compliance with the operational handbook."

The SFO responded, accepting some of the recommendations.[198]

Canada has had its difficulties with IMETS,[199] but the UK experience shows that appointing lawyers as case controllers is clearly not a *sufficient* condition for success, though (as with money laundering and organised crime), close liaison between lawyers and investigators at an early stage is vital to avoid wasted investigative effort, but only if the prosecutors themselves are clear and consistent, rather than having early advice from Case Controllers overruled by external counsel later. This is partly a quality of staff issue, but it is also one of prestige and power of external v internal counsel, and cost control. This is beyond the scope of this review to resolve.

---

[198] https://www.sfo.gov.uk/download/response-to-hmcpsi-case-progression-review-october-2019/

[199] see https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-vltn-ntgrtd-mrkt-nfrcmnt-2009-10/vltn-ntgrtd-mrkt-nfrcmnt-2009-10-eng.pdf ; https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/archive-vltn-nhncd-prtctn-2005-06/archive-imet-eipmf-eng.pdf; https://nationalpost.com/news/canada/white-collar-crime-task-force-doomed-to-failure-unless-separated-into-its-own-agency-retired-mountie; James W Williams, "Out of place and out of line: Positioning the police in the regulation of financial markets." *Law & Policy* 30, no. 3 (2008): 306-335; James Williams, *Policing the markets: Inside the black box of securities enforcement*. Routledge, 2012.

There is no equivalent separate institutional expertise for money laundering prosecutions. Some might be dealt with by the Serious Fraud Office or by the Financial Conduct Authority, but others (including HMRC tax cases) fall within the Crown Prosecution Service Organised Crime Strategy which aims to deliver cases and other interventions as follows:[200]

- By the Organised Crime Division of the CPS (OCD CPS), based in London, Birmingham and the North prosecuting Organised Crime cases directly investigated by the National Crime Agency;
- By the Complex Casework Units (CCU's) of the 13 CPS Areas prosecuting Organised Crime cases investigated primarily by Regional Organised Crime Units (ROCUs) and local Police Forces;
- By the 13 CPS Areas prosecuting Organised Crime cases investigated by local Police Forces; and
- By the International Division of the CPS working with OCD and NCA worldwide to better investigate and prosecute cases at source or in transit.

[200] https://www.cps.gov.uk/organised-crime-strategy

X. CONCLUSIONS AND REFLECTIONS

The 2018 FATF evaluation of the UK generated more data from different components of the complex AML regime in the UK than had been available previously, though the validity of these data is difficult to assess, with only modest published research. The UK does not lack rules and processes for dealing with suspicion and SARs, and in that sense the difference between common law and continental models may be exaggerated. Thus, there are significant legal constraints of intra-public sector communications (HMRC personal data on individual and business taxpayers to anyone) and public to private communications (police/NCA to private sector and individuals lack sufficient legal gateways for communication; the JMLIT is accessed by only a limited number of financial institutions). However, once a SAR has been made, there are few constraints from private to public, ever since the Drug Trafficking Offences Act 1986 made a first small breach in the dam of customer confidentiality by protecting banks from liability for making disclosures in suspected drug trafficking cases.[201] However, discretion continues to be a central feature of British policing and prosecutions, as does the decentralised/distributed nature of the loose-coupled AML process, in which the role of the FIU in developing investigations is less important than in some jurisdictions.[202]

One important feature of UK policing has been its flexible approach to the policing of the public sphere, with no firm line as to where the state ends and private collective or individual governance begins. Thus, an early study of data matching three decades ago showed the importance of large scale *private* sector data sharing in payment card fraud prevention,[203] later developing more broadly in public–private anti-fraud and counterfeiting efforts, including even the private sector financing of police units in the City of London police to deal with "organised" payment card fraud and insurance fraud cases (which otherwise would have received police and prosecution support only intermittently), under police command but with public–private joint steering committees on policy.[204] In the control of cybercrimes in many parts of the world, it is a

[201] Michael Levi, "*Pecunia non olet*: cleansing the money launderers from the Temple", *Crime, Law, and Social Change*, 16 (1991) 217–302; Michael Levi, "Pecunia non olet? The control of money-laundering revisited", in Frank Bovenkerk and Michael Levi (eds.), *The Organised Crime Community*, New York: Springer, 2007, pp. 161–182.
[202] See Eleanor Gale and Jessica Kelly, *Exploring the Role of the Financial Investigator,* Home Office Research Report 104, November 2018.
[203] Michael Levi, Paul Bissell and Tony Richardson, *The Prevention of Cheque and Credit Card Fraud,* CPU Paper 26, London: Home Office, 1991.
[204] Michael Levi, "Public and Private Policing of Financial Crimes: the Struggle for Co-ordination",

conscious strategy to extend the use of the private sector as part of "the policing family",[205] and also (in the UK) to recruit (or to seek to recruit) private sector experts as unpaid "special constables" to assist, at times, under-trained and (outside specialist units such as the National Crime Agency, Regional Organised Crime Units, and the National Cyber Security Centre) inexpert police. Alongside what has become known in the Netherlands, Sweden and, to a lesser extent, other parts of Europe generally as 'the administrative approach to organised crime', the successive Serious and Organised Crime Strategies of the UK government stress the importance of Protect and Prepare alongside the Pursue (law enforcement) function in the general ambition of harm reduction. There is no suggestion that these (and Prevent) are the exclusive roles of the public police.

Returning to AML, the UK (like the Netherlands) has always operated in a relatively high-volume reporting environment compared with other police FIU systems, and whatever the formal regulatory environment may be, even though they have been expanded somewhat following the criticisms in the 2018 Mutual Evaluation Report, the 124 (up from 80) or so – subject to recruitment issues under Covid-19 - UK FIU staff (in 2020) obviously cannot deal very comprehensively with all 478,437 SARs as well as carrying out the outreach and other activities required of them, especially given the complexity of many financial crime cases and of DAML requests. The AML regime of the UK and of other EU countries places significant demands on an ever-larger range of private sector actors, but the (subjective) 'appropriate balance' between public and private AML resources has not been the subject of clear public debate in the UK or in the national or international arenas such as the EU, FATF or UN. In this sense, the extension of the public into the private has crept upon us, just as the pervasive impact of private technology into the private sphere has. The FIU (and fraud investigation) resource scarcity long preceded the UK public

Journal of Criminal Justice and Security, 4 (2010) 343–357. See also https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/Pages/default.aspx.

[205] Michael Levi, Alan Doig, Rajeev Gundur, David Wall and Matthew Williams, "Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research", *Crime, Law and Social Change*, 67(1) (2017) 77–96. See also HMICFRS, *Fraud: Time to Choose. An inspection of the police response to fraud,* 2019. This is not only occurring in the UK but also internationally: see Benoit Dupont, "Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime", *Crime, Law and Social Change*, 67(1) (2017) 97–116; Benoit Dupont, "The global anti-cybercrime network", in Lennon Y.C. Chang and Russel Brewer (eds.), *Criminal Justice and Regulation Revisited: Essays in Honour of Peter Grabosky*, Abingdon: Routledge, 2018, p. 163; David Mussington, Brent J. Arnold, Benoit Dupont, Scott Hilts, Timothy Grayson, Christian Leuprecht, Liam Nevill, Brian O'Higgins and Josh Tupler, *Governing Cyber Security in Canada, Australia and the United States*, Centre for International Governance Innovation, 2018; Sanne Boes and E.Rutger Leukfeldt, "Fighting cybercrime: A joint effort", in Robert M. Clark and Simon Hakim (eds.), *Cyber-Physical Security*, Cham: Springer, 2017, pp. 185–203.

sector austerity programme, in which policing is not a protected area of public finance: but the reduction in UK police numbers has had an inevitable impact on financial investigation in practice, even though some investigation costs are recoverable from the government's Asset Recovery Incentivisation Scheme, making it profitable or at least cost-neutral for forces to devote some resources to them *provided this leads to actual proceeds of crime recoveries*.[206] This may be one reason why the number of accredited financial investigators has risen from 837 in 2004,[207] then mainly in the police and customs, to around 4,800 today, spread across 77 agencies[208] – though they may not all be currently engaged in financial investigation work. Nevertheless, a review of financial investigation by Gale and Kelly concluded:[209]

> "It also became apparent that there were challenges to the effective use of financial investigation, which were often systemic in nature. For instance, financial investigation was often considered and used as a tool for investigating economic crime and undertaking asset recovery only, despite the numerous benefits reported by both the FIs [financial investigators] and the non-FIs when it had been used during investigations of non-economic crime.
>
> This may be due to a limited understanding of financial investigation among key partners. The FIs reported that non-FI colleagues from their organisations as well as partners from the criminal justice system and other organisations sometimes lacked understanding of financial investigation. This could frustrate the progress of financial investigations – particularly the use of additional charges for money laundering and recovering criminal assets through confiscation."

Although a much broader problem than in the UK, which globally is a leader in sophisticated crime statistics, the lack of comprehensive and consistent statistics on the AML process has been noted by scholars and official bodies. The UK does not collect and never has collected systematically statistics on amounts in SARs and their conversion rate into subsequent action;

---

[206] This can have unintended impacts in skewing investigations towards cases where assets have not been dissipated or are more readily recoverable (i.e. are not overseas, and are in cash or other cheaply recoverable form: the Asset Freezing Orders make freezing easier and cheaper to administer, which will impact on recoveries). ARIS divides recovered assets between operational agencies and the Home Office on a 50/50 basis. While the Home Office portion of ARIS is earmarked as part of its core budget – making it a sort of hypothecated taxation – operational partners may use these funds as they see fit. Law enforcement agencies received a peak £72.9 million in 2015-6, and £48.3 million in 2019-20 from ARIS. See Home Office, Asset recovery statistical bulletin 2012/13–2017/18", Research Report 18/18, September 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/739567/asset-recovery-financial-years-2013-to-2018-hosb1818.pdf; *Asset Recovery Statistical Bulletin 2014/15 – 2019/20 England, Wales and Northern Ireland*, Home Office, 2020. There is, however, considerable attrition between the sums ordered to be confiscated and actual confiscation levels.

[207] Richard J Harding, *Evaluation of the Assets Recovery Agency training provision* (unpublished).

[208] Law Commission SARs Regime Consultation Review, 2018.

[209] Eleanor Gale and Jessica Kelly, *Exploring the Role of the Financial Investigator*, Home Office Research Report 104, November 2018, p. 43.

this is a hydraulic system in which it is arguable that one might as well have only the number of reports one is prepared to deal properly with, unless the system is *de facto* a mass dataset, which is a half-way house between an unusual transaction reporting model (Dutch-style) and a refined SAR system with far fewer reports but whose reports are more thoroughly followed up.[210] This has a "police culture" dimension, in that few investigators see it as a priority to tell the FIU when a SAR has been useful for either crime investigation or asset recovery purposes, and the FIU is too busy processing its vast volume of SARs to tell the private sector reporters, even when they are notified by LEAs, of how useful or otherwise the SAR has been. In more formal terms, the national College of Policing gives some guidance as to how to conduct financial investigation,[211] and Gale and Kelly make some recommendations,[212] as others have done before them about the plugging of intelligence gaps and better partnership work oriented towards disruption.[213] The lengthy Law Commission report does invite comments on the principal objectives of confiscation, but does not deal extensively with the policing issues.[214]

In a review that generally praises the UK's initiatives (whose outputs and outcomes often lie in the future, after the MER and the Plenary which awards its final grades), the FATF Mutual Evaluation Report criticises the UK's FIU for the absence of its own SAR follow-up investigation and for what may be described as the distributed model of sending out SARs and leaving it up to the individual recipients to investigate (or, more often, not to do so). The resource implications of giving the UK's FIU a much larger role in intelligence development have not been examined fully. (Although substantially more FIU staff have been promised - and some already employed - following the FATF report, as they were when the previous one was finalised in 2007). However, it is not clear that law enforcement would do much more with the intelligence if it was developed more fully by the FIU. (If nothing is actually done with it, what is the point of developing the SARs further?) This relative lack of follow-up is a problem with all forms of intelligence packages

[210] Michael Gold and Michael Levi, *Money-Laundering in the UK: an Appraisal of Suspicion-Based Reporting*, London: Police Foundation, 1994; Michael Levi, "Incriminating disclosures: an evaluation of money-laundering regulation in England and Wales", *European Journal of Crime, Criminal Law, and Criminal Justice*, 3(2) (1995) 202–217; Michael Levi, Peter Reuter and Terence Halliday, "Can the AML/CTF System Be Evaluated Without Better Data?", *Crime, Law and Social Change*, 69(2) (2018) 307–328.

[211] https://www.app.college.police.uk/app-content/investigations/investigative-strategies/financial-investigation-2/.

[212] Eleanor Gale and Jessica Kelly, *Exploring the Role of the Financial Investigator*, Home Office Research Report 104, November 2018.

[213] See Nick Maxwell and David Artingstall, *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime*, London: RUSI, 2017; Helena Wood, David Artingstall, Haylea Campbell and Anton Moiseienko, *Known Unknowns: Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers*, London: RUSI, 2018; and Nick Maxwell, *Future of Financial Intelligence Sharing (FFIS) research programme 'Five years of growth in public–private financial information-sharing partnerships to tackle crime'*, RUSI, 2020.

[214] Law Commission, *Confiscation of the Proceeds of Crime*, 2020.

to and by the NCA and its predecessor agencies,[215] and it is also true of the centralised fraud reports made to Action Fraud and (after filtering for expected investigatability) distributed on to forces around the country by the National Fraud Intelligence Bureau in the City of London Police.[216] As elsewhere (including Canada), there is simply far too much "intelligence" around from which to develop Pursue actions, whether because of limited personnel or of cross-border obstacles, which include overburdened FIUs elsewhere and domestic political resistance to serving the interests of foreign states when their own domestic cases cannot be investigated and there are other needs expressed by their citizens and politicians.[217] This is a problem in all jurisdictions, even in "legality principle" ones where there is an obligation to prosecute once there is 'sufficient' evidence; the broader question of how much expenditure on financial investigation – or indeed expenditure on the criminal prosecution of money laundering or any other offence – is socially optimal is out of scope for this report, but is an important one for Canada and all countries. There are also serious limits from austerity to prosecutors' resources in cases high and low, both in the UK and elsewhere, even in North America. The implications of these practical limitations of criminal justice outputs for the earlier stages of AML system as a whole remain inchoate and have not been considered seriously.[218]

The Executive Summary of the FATF report on the UK states, positively:[219]

> "*Overall Level of Compliance and Effectiveness …*
>
> 4. The UK has implemented an AML/CTF system that is effective in many respects. Particularly good results are being achieved in the areas of investigation and prosecution of ML/CTF, confiscation, the implementation of targeted financial sanctions related to terrorism and

[215] Michael Levi and Mike Maguire, "Something old, something new; something not entirely blue: Uneven and shifting modes of crime control", in Tim Newburn and Jill Peay (eds.), *Policing: Politics, Culture and Control*, Oxford: Hart Publishing, 2012, pp. 195–218.
[216] Alan Doig and Michael Levi, 'Editorial: The dynamics of the fight against fraud and bribery: reflections on core issues in this PMM theme', *Public Money and Management*, 40:5, 343-348; Alan Doig, "Fraud: from national strategies to practice on the ground – a regional case study", *Public Money & Management*, 38(2) (2018) 147–156; Michael Levi and Alan Doig, "Exploring the 'Shadows' in the Implementation Processes for National Anti-fraud Strategies at the Local Level: Aims, Ownership, and Impact", *European Journal on Criminal Policy and Research* (2020) 26: 313–333; Home Affairs Select Committee, *Policing for the* Future, HC 515, 2018; Michael Skidmore, Josephine Ramm, Janice Goldstraw-White, Clare Barrett, Sabina Barleaza, Rick Muir and Martin Gill, *More Than Just A Number: Improving the Police Response to Victims Of Fraud*, London: Police Foundation, 2018; HMICFRS, *Fraud: Time to Choose. An inspection of the police response to fraud,* 2019.
[217] Though initially rebuffed when this author proposed it in 2001, the funding of a police and then NCA overseas corruption unit by the UK Department of International Development was an important development in ensuring more attention to overseas corruption cases than would have been possible in practice. See Jackie Harvey, "Tracking the international proceeds of corruption and the challenges of national boundaries and national agencies: the UK example." *Public Money & Management* 40, no. 5 (2020): 360-368. The NCA Annual Report noted that the International Corruption Unit (ICU) within the NCA restrained or detained £32m of funds in 2019/20; a further £146m has been confiscated or forfeited, of which £139m has been returned to developing countries.
[218] We are not arguing that such a pursuit of every case would be a fiscally sensible policy.
[219] FATF, *Mutual Evaluation Report – UK*, 2018, p. 6.

proliferation, protecting the non-profit sector from terrorist abuse, understanding the ML/CTF risks facing the country, preventing misuse of legal structures and co-operating domestically and internationally to address them. However, major improvements are needed to strengthen supervision and implementation of preventive measures, and ensure that financial intelligence is fully exploited.

5. In terms of technical compliance, the legal framework is particularly strong with only two areas in need of significant improvements—measures related to correspondent banking and the UKFIU.
6. The UK has significantly strengthened its AML/CTF framework since its last evaluation particularly in relation to operational co-ordination among law enforcement agencies, stronger investigative tools, mechanisms to facilitate public/private information sharing, and the creation of an authority to address inconsistencies in the supervision of lawyers and accountants. One important issue which is outstanding from the previous assessment is the need to enhance the resources and capabilities available to the UKFIU."

The issue of *effectiveness at what* is not addressed, and the report stays at the level of activity indicators, as is the case generally with such reports.[220] The metrics of success remain under-explored, nor is the proportionality of reporting issue tackled other than by assertion, for example: "there remains an underreporting of suspicious transactions by higher risk sectors such as trust and company service providers (TCSPs), lawyers, and accountants."[221] What actually would or should happen to those deemed sectorally risky in the aftermath of these extra exhorted reports remains an intellectual work in progress. The scalability of the JMLIT for dealing with larger numbers of cases than the (undeclared) number currently done remains an open question that has not been publicly examined.

The UK is serious about its major crime control and national security objectives and aims to make progress against identified social harms, using AML as one of several mechanisms to reduce crimes and the harms from them. Its offshore roles and relationships are a legacy of Empire, and they have not been considered here, but they continue to shape the perception of the UK externally and are a source of tension within the UK government and between it and the Overseas Territories and Crown Dependencies. The compliance function of the private sector has been transformed into an ally of policing by a combination of criminal and regulatory threats and

[220] In its one-page statement in December 2019, the Wolfsberg Group expressed its frustration at the lack of developed thinking on effectiveness: see https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Effectiveness%201%20pager%20Wolfsberg%20Group%202019%20FINAL_Publication.pdf .

[221] Ibid, p. 6.

recommendations, and the long tradition of public–private cooperation in the UK[222] has been deployed to make this a collaborative as well as top-down endeavour. The effects of these actual and prospective changes on crime rates and harms remains under-explored, and the FinCEN leaks coverage continues to throw an unflattering light upon them: but this seems not to have inhibited this inexorable trend towards "responsibilisation" of the private sector to play public roles, even if implementation test mechanisms like mystery shopping have not yet been systematically deployed in the thematic reviews that have become part of the regulatory toolbox. Brexit will have an impact on the international networking process, and access to Europol: the clunky Council of Europe Mutual Legal Assistance mechanisms have been allowed to get rusty and despite improvements, Egmont has accounted for the majority of inter-FIU exchanges (see Table 3), and in the past year surged in popularity, while exchanges via the EU (including the FIU.Net at Europol) fell significantly. The explanation for these changes is out of scope and less salient for the Canadian readership. But many of the issues raised in this review will still be able to operate relatively unimpeded.

The technological features of the electronic database ELMER have been in need of refashioning for well over a decade – this author began a review of it two decades ago - but this is a difficult time for costly changes, and the government seeks private sector hypothecated contributions from an Economic Crime Levy, which is currently out for consultation. Whether Covid-19-racked and post-Brexit Britain will have economic strains that tempt more organisations to launder money and more private sector enterprises to protest about their own *over*-investment and public *under*-investment in action on SARs remains to be seen. Hitherto, apart from specialist concern about de-risking of customers, correspondent banking facilities, and Global South nations as an unintended counter-productive consequence of AML regulation, there has been little sustained popular or political protest about the social, economic or privacy costs of AML in the UK. So unless there is a determined shift in the direction of travel of AML in the UK – rare in the aftermath of a positive AML Mutual Evaluation Report – or a shift in thinking by the FATF itself as part of its self-review in 2020, the most likely future direction is more of the same, with some additional attention being paid to the areas such as FIU investigation levels and its outdated technological systems on which the MER recommends the need for improvement. All national systems have adapted to high-level sanctions-backed 'recommendations' from FATF and from other bodies over the last three decades. They generally are grafted on to loose-coupled systems of private and public intelligence, investigation, regulation and prosecution systems in ways that

[222] Sir Robert Peel's 1829 principle that "the police are the public and the public are the police" was a very different model from the Continental models.

are seldom clear and entail often implicit rather than explicit resource allocation tensions. In some jurisdictions (Canada included) these have given rise to constitutional decisions, and in all they involve clashes between the tectonic plates of data protection and data sharing, most sharply in the European Union.[223] Scandals and Commissions give an opportunity to rethink these linkages and the boundaries of interventions nationally and internationally. It is hoped that in reviewing the UK, this report will give some more general insights upon which the Cullen Commission can draw.

[223] Ben Vogel and Jean-Baptiste Maillart (eds.) *National and International Anti-Money Laundering Law: Developing the Architecture of Criminal Justice, Regulatory Law and Data Protection*, The Hague: Intersentia, 2020.