Written Evidence Submitted by Professor Nic Ryder (Cardiff University), Dr Samantha Bourton (University of the West of England, Bristol) and Dr Fiona Brimblecombe (The University of Manchester) (ECCTB30)

Public Bill Committee Call for written evidence: Economic Crime and Corporate Transparency Bill

Introduction to Authors

Professor Nic Ryder has conducted financial crime research and has played an advisory role both nationally and internationally. His research has focused on money laundering, terrorism financing, fraud, and corporate economic crime with reference to the exchange of information. Dr Sam Bourton is a Lecturer in Law at the University of the West of England. Sam's research interests lie in the law of financial crime, particularly, the law pertaining to tax evasion and money laundering. She regularly publishes and presents her research in these areas. Dr Fiona Brimblecombe is a Lecturer in Law at the University of Manchester, and her research focuses on personality rights in the internet age, including the 'right to erasure' in the GDPR, misuse of private information, defamation, and the exchange of information.

Executive Summary

This submission concentrates on Clauses 148 to 153 of the Economic Crime and Corporate Transparency Bill, which concern disclosures to prevent, detect or investigate economic crime. The first section of the submission briefly identifies the importance of private sector information exchange in the detection of financial crime, while the second section provides an overview of existing legal gateways. The third section of the submission identifies the improvements made by the Bill to the existing legal framework and identifies its remaining weaknesses, making associated recommendations for improvement. While the Bill concentrates on the exchange of information between private regulated entities, the final section of this submission critiques the current exchange of information mechanisms between Law Enforcement Agencies in the United Kingdom through the presentation of a case study.[1] The case study will serve to demonstrate that, in practice, there are inherent flaws in the ability of LEAs to obtain and exchange of information to detect and address financial crimes.

[1] Hereinafter 'LEA' and 'UK.'

Accordingly, the final section provides recommendations for reform, which extend beyond private sector information sharing.

Private Sector Exchange of Information

1. The Financial Action Task Force has noted that 'effective information sharing is one of the cornerstones of a well-functioning AML/CFT framework.'[2] Indeed, the importance of information sharing has been demonstrated by the Joint Money Laundering Intelligence Taskforce, which was established as a private/public partnership between LEAs and the financial sector.[3] Information sharing through JMLIT is enabled by pre-existing statutory provisions introduced by the Crime and Courts Act 2013, which permits reporting entities to act as information gateways to facilitate the exchange of information between the private sector and LEAs.[4] The FATF has described this as a 'strong feature of the system … [that] enables any person across the public or private sector to voluntarily share information with the NCA'.[5] JMLIT 'made very quick progress in aiding voluntary information sharing … and has quickly demonstrated [its] … benefits'.[6] It has enabled the UK to become a global leader in the exchange of information between reporting entities and LEAs. For example, the UK model has been adopted in Australia,[7] Singapore,[8] and Hong Kong.[9] Indeed, the FATF noted, 'JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015 and is considered to be an example of best

[2] Financial Action Task Force, *Private Sector Information Sharing* (Financial Action Task Force 2017) 2. Hereinafter 'FATF'.
[3] National Crime Agency, 'National Economic Crime Centre', (n/d) available from <www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed September 27 2021. Hereinafter 'JMLIT'.
[4] Crime and Courts Act 2013, s 7.
[5] Financial Action Task Force *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant* (Financial Action Task Force 2015) p 5.
[6] Financial Conduct Authority, 'Effectiveness and proportionality: our financial crime priorities – speech by Rob Gruppetta, Head of Financial Crime Department' (November 10 2016) available from <www.fca.org.uk/news/speeches/effectiveness-proportionality-financial-crime-priorities> accessed 14 February 2019.
[7] AUSTRAC, 'Fintel Alliance', (n/d) available from <www.austrac.gov.au/about-us/fintel-alliance> accessed February 2019.
[8] Monetary Authority of Singapore, 'CAD and MAS partner industry stakeholders to fight financial crimes' (April 24 2017) available from <www.mas.gov.sg/News-and-Publications/Media-Releases/2017/CAD-and-MAS-Partner-Industry-Stakeholders-to-Fight-Financial-Crimes.aspx>, accessed February 17 2019.
[9] Hong Kong Monetary Authority, 'Fraud and Money Laundering Intelligence Taskforce launched' (May 26 2017) available from <www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml> accessed February 2 2019.

practice'.[10] Accordingly, the aim of Part 5 of the Bill, in focusing on improving the legal framework relating to the exchange of information between the regulated sector for the purposes of combatting economic crime, is commendable.

2. Presently, the exchange of information for AML/CFT purposes in the private sector is primarily facilitated by s.339ZB of the Proceeds of Crime Act 2002, which permits 'voluntary disclosures within the regulated sector'.[11] POCA allows the regulated sector to 'share information with each other on a voluntary basis in relation to suspected instances of … money laundering and/or terrorist financing'.[12] Information sharing can either be instigated by the regulated sector or the National Crime Agency (NCA).[13] However, before an institution can make a disclosure, it is required to notify a NCA authorised officer.[14] Regulated institutions are also permitted to submit joint disclosure reports, otherwise known as 'Super SARs', following information exchange.[15] Super SARs were introduced to remedy some of the deficiencies in the Suspicious Activity Reports regime, which is widely regarded as deficient, especially owing to its serious absence of rapid triage, dissemination, evidential gathering processes, the inability to cope with the large volumes of SARs, compliance costs and inadequate exchange of information mechanisms.[16] SARs are under-utilised, the system suffers from poor management information on how the reports are used,[17] and as a result has been an increase in the number of SARs submitted to the NCA. The trend has remained upwards in subsequent years, with the Financial Intelligence Unit receiving 573,085 SARs in 2020.[18] Super SARs were intended to provide the NCA with fewer, more valuable, SARs, by capturing comprehensive criminal intelligence from a number of sources. However, a number of factors presently inhibit information sharing within the regulated sector. Some of these concerns are addressed by the Bill, yet significant weaknesses remain, as outlined below.

---

[10] Financial Action Task Force, *Anti-Money Laundering and Counter-Terrorist Financing Measures: United Kingdom Mutual Evaluation Report* (Financial Action Task Force 2018) 6.
[11] Criminal Finances Act 2017, s 11. This Act introduced this measure into the Proceeds of Crime Act 2002, s 339ZB–ZG and the Terrorism Act 2000, s 21CA–CF. Hereinafter 'POCA'.
[12] Home Office, *Home Office Circular: Criminal Finances Act 2017 Money Laundering: Sharing of Information within the Regulated Sector Sections 339ZB-339ZG* (Home Office 2018) 1.
[13] Ibid.
[14] Proceeds of Crime Act 2002, s 339ZB(4).
[15] Law Commission, *Anti-Money Laundering: The SARs Regime Report* (Law Com No 384, 2019) 44.
[16] See above n 10. Hereinafter 'SARs'.
[17] See above n 15.
[18] National Crime Agency, *SARs Annual Report 2020* (National Crime Agency 2020) 4. Hereinafter 'FIU'.

Clauses 148-153 - Disclosures to prevent, detect or investigate economic crime etc.

3. Clause 148, Part 5 of the Bill relates to direct disclosures where there are no breaches of confidences. This accords with one of the central objectives of the Bill, according to the Explanatory notes – 'Enabling businesses in certain sectors to share information more effectively to prevent and detect economic crime.'[19] Under this clause, a disclosure can be made that does not breach an obligation of confidence from person A to person B,[20] if they are carrying out business in the regulated sector[21] (such as businesses providing financial services or independent legal services) if B is also carrying on business in a related sector.[22] This information would pertain to a former or a current customer of A's, that may 'assist' B.[23] The disclosure has to have been made at the request of B or form part of a warning regarding financial crime from A to B.[24]

4. The result of this clause is that it will likely encourage business in the regulated sector to disclose information about former/current customers that they suspect of having links to financial crime without feeling constrained by concerns relating to confidentiality and data protection law.[25] This clause, while providing welcome protection for regulated-sector businesses disclosing information concerning customers relating to economic crime, balances this protection for businesses regarding disclosure with the principles of proportionality and data minimisation.[26] It does this through the caveats of a 'warning condition' or a 'request condition' as present.[27] In practice, this may mean that business A must feel sufficiently strongly that they must disclose the information as a *warning* to business B (due to the potential threat of economic crime), or business B may have reason to suspect that illicit activity could be linked sufficient to *request* information about a particular customer. There is the additional safeguard that Clause

[19] Economic Crime and Corporate Transparency Bill, Explanatory Notes, 9. Accessible at: https://publications.parliament.uk/pa/bills/cbill/58-03/0154/en/220154en.pdf
[20] Section 148(1), Part 5, Economic Crime and Corporate Transparency Bill 2022.
[21] Ibid, 148(2).
[22] Ibid, 148(1)(b) and (3).
[23] Ibid, 148(1)(e).
[24] Ibid, 148(1)(d).
[25] Ibid, 148(9).
[26] See the white paper by Bourton, Ryder and Brimblecombe Part 1, Accessible at: https://synalogik.com/white-papers/.
[27] Section 148(3) and (4) Part 5, Economic Crime and Corporate Transparency Bill 2022.

148 only applies to businesses in the *regulated sector*,[28] which are particularly at risk of being targeted in financial crime, and best placed to spot early warning signs that illegal activity is present.

5. Clause 149, Part 5 of the Bill concerns indirect disclosures of information with no breach of confidence. Here, a disclosure by person A to person B does not breach any obligation of confidence if the information relates to a customer/former customer[29] and due to concerns about economic crime, A has decided to 'terminate relationships' with that customer, refuse them products/services or to restrict their product access.[30] This is an inbuilt safeguard to balance the importance of information reporting against confidentiality; business A must have more than a vague suspicion that the customer in question is linked to financial crime – they must be sufficiently concerned that they have *acted against* the customer/former customer in restricting their access to products *due to this.* This, by proxy, raises the 'seriousness threshold' before a disclosure under s.149 would take place. This clause also has a narrow reach: it encompasses business that take deposits, electronic money, payment institutions, are a cryptoasset exchange provider or are custodian wallet providers.[31] The result is that Clause 149 only applies to certain types of business who are likely to handle large sums of money and are particularly at risk of being targeted by white collar criminals; this section does not therefore operate as a carte blanche for other types of business to utilise this disclosure mechanism. Existing data protection law also operates here as an additional safeguard to relevant disclosures if the information is personal data.[32] For a discussion of the current data protection landscape relating to disclosures and financial crime, see the briefing paper of Bourton, Ryder and Brimblecombe.[33]

Strengths of the Bill

6. Clause 148 enables information sharing within the regulated sector either upon request, or spontaneously, the latter following 'safeguarding action' by the transmitting

[28] Ibid 148(2). There is also the ability of the Secretary of State to add businesses of a certain description to this section's application by additional Regulations accompanying the Bill if it becomes an Act under 2(b).
[29] Ibid 149(2)(b).
[30] Ibid 149(2(c).
[31] Ibid 149(3).
[32] Ibid 149(2)(e).
[33] Part 1, Accessible at: https://synalogik.com/white-papers/.

institution.[34] Unlike s.339ZB of POCA, there is no requirement for either institution to notify the NCA before a disclosure is made.[35] This is a welcome development, for the current procedure is complicated and may cause delays, discouraging businesses from exchanging information or exposing them to the risk of legal action.[36] Clause 148 enables a business in the regulated sector to exchange information upon request, if supplying the information would assist the requesting institution in carrying out 'relevant actions'.[37] Clause 151 identifies relevant actions, all of which must be undertaken for the purposes of "preventing, detecting or investigating economic crime".[38] In taking a broad approach, the Bill avoids replicating the unsatisfactory former focus on suspicions of AML/CFT as a condition for information exchange. The benefits of incorporating predicate offences into financial intelligence and information exchange provisions in their own right is demonstrated by the failure to report fraud in the UK.

7. If a suspected fraud is committed against a reporting entity it must be reported to its Money Laundering Reporting Officer,[39] followed by the NCA. The primary statutory obligation for reporting instances of fraud is contained under the POCA 2002 and successful fraud is defined as money laundering for the purpose of this Act.[40] However, there is no legal obligation to report unsuccessful or attempted frauds to the NCA because any attempted frauds will not give rise to any criminal proceeds and therefore fall outside the scope of the SARs regime. As a result, 'fraud is massively underreported'.[41] In order to address this deficiency, the Fraud Review recommended that businesses and individuals could report fraud to the National Fraud Reporting Centre.[42] This recommendation resulted in the creation of the National Fraud Intelligence Bureau,[43] an agency dedicated to analysing and assessing fraud with the

[34] Economic Crime and Corporate Transparency HC Bill (2022-23) [154], cl 148(3)-(4).
[35] Proceeds of Crime Act 2002, s.339ZB(4).
[36] See for instance, *Lonsdale v National Westminster Bank Plc* [2018] EWHC 1843 (QB); *Shah v HSBC Private Bank Ltd* [2012] EWHC 1283; [2013] 1 All ER (Comm) 72.
[37] Economic Crime and Corporate Transparency HC Bill (2022-23) [154], cl 148(3).
[38] Ibid, cl 151(a).
[39] Hereinafter 'MLRO.'
[40] It is important to note that the Proceeds of Crime Act 2002, s.340 applies to all criminal conduct, which includes fraud.
[41] Attorney General's Office, *Fraud Review: Final Report* (Attorney General's Office 2006) 7.
[42] Ibid.
[43] Hereinafter 'NFIB.'

aid of analysts from both LEAs and the private sector.[44] The NFIB, or Action Fraud, was managed by the City of London Police and by the Home Office.[45] However, Action Fraud was abolished following an investigation by The Times which illustrated how the organisation's staff were trained to mislead victims of fraud that their cases were being investigated.[46] The Times reported that fewer than two percent of reports submitted resulted in an arrest and fewer than one percent of police officers were assigned to fraud investigations. Consequently, the Home Office commissioned a review of how fraud is policed, which concluded that the police are not adequately prepared to tackle fraud.[47] In July 2021, HM Government announced that Action Fraud was to be abolished and placed within the NCA.[48]

8. By enabling private sector information exchange for the purposes of "preventing, detecting or investigating economic crime", Clause 148 may help to provide additional intelligence relating to predicate offences, such as fraud. However, we also recommend that the reporting of unsuccessful frauds to the NCA should become mandatory. There are advantages to adopting this approach – it will lead to an enhanced understanding of fraud, and result in better intelligence for policing fraud.

Remaining Weaknesses

9. At face value, Clause 148 ostensibly applies to the entirety of the regulated sector. This is a positive development, for previous private sector information exchange initiatives have focused on the financial services sector. However, it will be important to ensure that the terms of the statute are not restricted in practice, as is the case with the current s.339ZB of POCA. Indeed, whilst s.339ZB appears to apply to the whole regulated sector, Home Office Guidance and NCA practice restrict the regime to financial and credit institutions.[49] This significantly restricts the dissemination of intelligence relating

[44] ibid at 10.
[45] A Palmer, *Countering Economic Crime: A Comparative Analysis* (Routledge 2018) 46.
[46] M Morgan-Bentley, 'Action Fraud Scrapped after Time Expose' The Times (July 28 2021) available from <https://www.thetimes.co.uk/article/fraud-line-scrapped-after-times-expose-n2tlkbmrv> accessed 26 April 2022.
[47] Craig Mackey and Jerry Savill, *Fraud A Review of the National 'Lead Force' Responsibilities of the City of London Police and the Effectiveness of Investigations in the UK* (City of London 2020).
[48] HM Government, *Beating Crime Plan – Fewer Victims, Peaceful Neighbourhoods, Safe Country* (HM Government 2021) 2. Hereinafter 'HMG'.
[49] Home Office, 'Circular 007/2018: Criminal Finances Act: Sharing Information within the Regulated Sector (1st February 2018) <https://www.gov.uk/government/publications/circular-0072018-criminal-finances-act-sharing-information-within-the-regulated-sector> accessed 22 November 2022; National Crime Agency, 'Required Notification under s.339ZC of Proceeds of Crime Act 2002' <https://www.nationalcrimeagency.gov.uk/what-we-

to economic crime and limits the availability of Super SARs to enhance the current system. Accordingly, we recommend that Clause 148 is applied to the entirety of the regulated sector, as currently drafted. In addition, s.339ZB of POCA should be applied to the entirety of the regulated sector, or, preferably, a clause similar to s.339ZD of POCA should be added to the Bill, to facilitate the disclosure of Super SARs. Moreover, notwithstanding the acclaim it has enjoyed, the composition of JMLIT should be extended. The FATF has noted that 'some stakeholders felt disenfranchised by their exclusion from it. Many felt that … JMLIT [should be] expanded [to allow] greater dissemination of information'.[50] At present, JMLIT does not engage with reporting entities that are particularly vulnerable to abuse by money launderers. It seemingly focuses exclusively on working with the financial services sector while ignoring other professions, such as accountants,[51] lawyers,[52] and estate agents.[53] The Law Commission concluded that the JMLIT's remit should be extended to include a broader range of reporting entities from the entire regulated sector in order to 'provide a better understanding of relevant intelligence through the sharing of information across multiple sectors'.[54] In response, the NCA stated, 'we do not believe that a simple expansion of the current JMLIT would be … effective'.[55] Conversely, the City of London Police suggested that the JMLIT could contain a number of 'sub-sets … concentrating on different sectors thereby allowing full access or the ability for the JMLIT to co-opt additional members'.[56] Although the creation of the JMLIT and the resultant information sharing has achieved some notable successes, it now seems necessary for HMG to widen the scope of the information sharing model to include other industries, such as social media platforms.[57]

---

do/crime-threats/money-laundering-and-illicit-finance/required-notification-under-s-339zc-of-proceeds-of-crime-act-2002> accessed 22 November 2022.

[50] See above, n 5 at 165.

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

[52] Ibid chapter 7. See also Financial Action Task Force, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (Financial Action Task Force 2013).

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

[54] See above n 15 at 174.

[55] Ibid at 44.

[56] Ibid at 166.

[57] Nicholas Ryder, 'Cryptoassets, Social Media Platforms and Defence against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown' (2020) 8 Journal of Business Law 668, 687-692.

10. Clause 148 only authorises the exchange of information on request, or spontaneous exchange following 'safeguarding action' being taken against a customer.[58] The drawbacks of a system based on requests have been identified in other areas of financial crime prevention, such as the international exchange of information in tax matters, which has evolved into an automatic exchange of information system.[59] Here, information exchange was inhibited by the fact that countries would need to illustrate that misconduct or noncompliance had taken place in order to make a request for tax-related information, yet it would often need to make the request to obtain this information, effectively leaving them in a 'Catch-22' situation.[60] Regulated institutions may face similar issues when required to establish their reasons for believing that another institution holds information relating to relevant actions before making a request, if receiving institutions interpret this requirement too strictly.[61] While a system of automatic exchange of information is inappropriate in this context, additional guidance, as well as an effective system of spontaneous information exchange, would alleviate some of these concerns. However, as presently drafted, Clause 148 provides that regulated institutions can only spontaneously exchange information following 'safeguarding action'.[62] This means that the suspicion of the regulated institution must be crystallised, and a SAR must be submitted, before spontaneous information exchange. This prevents the submission of Super SARs, designed to enhance the SAR system, and severely limits information exchange in practice. On the other hand, as noted above, the requirement of taking safeguarding action helps to balance the need for disclosure by businesses with the principles of proportionality and data minimisation. Accordingly, the need to protect the right to privacy and use of personal data may appropriately set limits on the scope of information exchange.

[58] Economic Crime and Corporate Transparency HC Bill (2022-23) [154], cl 148(4)-(5).
[59] International Tax Compliance Regulations 2015, SI 2015/878 (as amended by SI 2017/598, SI 2020/438, and SI 2020/1300); OECD, *Standard for Automatic Exchange of Financial Account Information in Tax Matters* (2nd edn, OECD 2017).
[60] McIntyre likened the prohibition to requiring that fishermen know the name of a fish, or its identifying tag, before being able to catch it, 'The only reason I can imagine for wanting to put such a ridiculous limitation on fisherman would be to keep them from catching fish.' MJ McIntyre, 'How to End the Charade of Information Exchange' [2009] Tax Notes International 255, 257.
[61] Economic Crime and Corporate Transparency HC Bill (2022-23) [154], cl 148(3)(b).
[62] Ibid, cl 148(4)-(5).

Public Sector Exchange of Information

11. Although the Bill focuses on the exchange of information between private regulated entities, the researchers also note that there are significant weaknesses in the exchange of information between public law enforcement authorities, which are also in need of rectification. To evidence this statement, the researchers have provided a case study below, on Her Majesty's Revenue & Customs' failure to exchange information related to terrorism financing to the UK Security Services and makes associated recommendations.[63]

Terrorism Financing

12. HMRC connected Shahzad Tanweer, one of the July 2005 terrorists, with a suspected VAT fraud, yet the information was not disclosed to the Security Intelligence Service (SIS).[64] The group linked to Tanweer gained £8bn from fraud, of which it sent '£80 million to al-Qaeda'.[65] There are legislative mechanisms that facilitate the exchange of information between HMRC and SIS.[66] However, HMRC officials 'were prevented from sharing intelligence … due to its desire to keep tax records confidential'.[67] The reluctance to exchange the information contradicts the legislation and this could be associated not with the legislation or guidance, but the restrictive interpretation of 'taxpayer confidentiality', which limits the ability of HMRC to exchange information.[68]

---

[63] A detailed report on these case studies was submitted to the Committee by the authors in October 2022. Hereinafter 'HMRC'.

[64] It has been suggested that HMRC became aware of the tax fraud scheme as early as 1995. See Tom Harper and Mark Macaskill, 'Glaswegian in £300m Fraud Linked to Bin Laden' The Times (London, April 14 2019) available from <https://www.thetimes.co.uk/article/glaswegian-in-300m-fraud-linked-to-bin-laden-x707d09pk?region=global> accessed August 19 2022.

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

[66] See for example the Anti-terrorism, Crime and Security Act 2001, HMRC Information Disclosure 19 Guide (IDG50140) and the Counter Terrorism Act 2008.

[67] Ibid.

[68] Further restrictions are imposed by the Commissioners for Revenue and Customs Act 2005 (CRCA), which provides that information must not be disclosed to anyone unless the person making the disclosure has the authority to do so. This applies to HMRC providing information to government departments, LEAs, and other public bodies. However, this restriction does not apply if the disclosure is 'made for the purposes of a criminal investigation or criminal proceedings relating to a matter in respect of which the Revenue and Customs have functions.' HMRC's duty of confidentiality is also 'subject to any other enactment permitting disclosure', and many legal gateways have been enacted to provide for the exchange of information between HMRC and LEAs. The Counter Terrorism Act 2008 provides that 'a person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions'. Interestingly, HMRC also has a 'duty to co-operate' and 'disclosure' under the Money Laundering Regulations, which provide that 'co-operation may include the sharing of information which the supervisory authority is not prevented from disclosing'.

13. Secondly, prior to the terrorist attacks in June 2017, Khuram Butt one of the terrorists, was investigated and arrested on suspicion of falsely reporting fraudulent activity on three bank accounts.[69] Butt was alleged to have made 'unauthorised withdrawals from his accounts and pocketing the refunds'.[70] Furthermore, had successfully applied for two online loans totalling £14,000.[71] After his arrest, Butt was granted bail and the fraud charges were dropped due to insufficient evidence.[72] Santander were under no legal obligation to exchange the information or to report the suspected fraud committed by Butt.[73]

14. Thirdly, due to the limitations of the SARs regime, student loans are a perfect mechanism to fund acts of terrorism.[74] In order to fund the terrorist attack in the Manchester Arena, Salman Abedi misused his student loans.[75] Abedi received £7,000 from the Student Loans Company after securing a place on a degree at Salford University in October 2015.[76] The SLC paid £1,000 in to Abedi's account at the start of January 2017 and a further £2,258 at the end of that month.[77] Abedi continued to receive funds from the SLC even though he had stopped attending classes.[78] The SARs regime only applies to the regulated sector, and as such, Higher Education Institutions

---

[69] See Mark White 'London Bridge Attack: MI5 Accused of "Damning List" of Failures', Sky News (June 28 2019) available from <https://news.sky.com/story/london-bridge-attack-mi5-accused-of-damning-list-of-failures-11750204>, accessed August 16 2022 and Intelligence and Security Committee, *The 2017 Attacks: What Needs to Change? Westminster, Manchester Arena, London Bridge, Finsbury Park, Parsons Green* (Intelligence and Security Committee 2018) 85.

[70] London Bridge Inquests, 'Inquests Concerning the Attackers Day 6A' (July 9 2019), available from <https://londonbridgeinquests.independent.gov.uk/wp-content/uploads/2019/07/LBI-Day-6A.pdf> accessed August 16 2022.

[71] Ibid 42, 43, 66 and 67.

[72] Ibid at 41. Also see above n 69 at 85.

[73] See Janice Goldstraw-White and Martin Gill, The Mandatory Reporting of Fraud: Finding Solutions and Sharing Best Practice (Fraud Advisory Panel 2021). Rashid was convicted of two counts of preparing acts of terrorism under the Terrorism Act 2006, s. 5(1)(b).

[74] Any new full-time student in the UK can apply for a Maintenance Loan, which is paid directly into the student's bank account. See HM Government 'Student Finance', (n/d) available from <https://www.gov.uk/student-finance/new-fulltime-students> accessed June 19 2022. See *R v. Yahya Rashid* [2016] EWCA Crim 568.

[75] Robert Mendick, 'Exclusive: Manchester Suicide Bomber Used Student Loan and Benefits to Fund Terror Plot', The Telegraph (London May 27 2017) available from <https://www.telegraph.co.uk/news/2017/05/26/exclusive-manchester-suicide-bomber-used-student-loan-benefits/> accessed June 19 2022. An investigation by the European Commission estimated that Abedi had received up to $18,000 in student loans and other benefit payments. See European Commission, *Study on an EU Initiative for a Restriction on Payments in Cash* (European Commission 2017) 48.

[76] Ibid (European Commission) at 48. Hereinafter 'SLC'.

[77] Peter Stubley, 'Hashem Abedi Trial: Benefits Claimed by Manchester Bomber's Family Were Used in Terror Plot Jury Hears' The Independent (February 10 2020) available from <https://www.independent.co.uk/news/uk/crime/manchester-arena-bombing-benefits-family-samia-abedi-hashem-trial-a9327816.html> accessed June 19 2022.

[78] See above n 75 at 50.

(HEIs) would not fall within this definition.[79] However, could HEIs fall within the definition of a High Value Dealer for the SARs regime to apply?[80] A survey of the application of the SARs regime on HEIs noted that only 2 out of 110 respondents considered themselves to be high value dealers.[81] Accordingly, the HEI attended by Salman Abedi was under no obligation to submit a SAR to the NCA under the Money Laundering Regulations, although it may have had a duty to report by virtue of its authorisation with the Financial Conduct Authority.

Conclusion

15. Of course, information sharing and increased co-operation can result in more comprehensive financial profiles of customers that enable financial investigators to focus on certain financial instruments and transactions. However, it must be remembered that the mechanisms provided for in Clauses 148 and 149 are voluntary and reporting entities can decline an invitation to exchange. Therefore, if the Act is not clear in enabling information exchange and protecting the regulated sector from adverse legal, financial, and reputational consequences, then the regulated sector is likely to err on the side of caution and refuse to exchange information, inhibiting the detection of economic crime. Accordingly, the researchers have made the following recommendations to improve Clause 148 of the Economic Crime and Corporate Transparency Bill, as well as recommendations to improve the exchange of information relating to financial crime more generally.

Recommendations

16. This submission has demonstrated that there are inherent flaws in the UK's ability to ensure the exchange of information. To remedy the weaknesses identified, a range of reforms could be introduced:

- Clause 148 of the Bill should be applied to the entirety of the Regulated Sector, as currently drafted. It is important to ensure that the legal gateway created by the Bill is

[79] The Money Laundering, Terrorist Financing Transfer of Funds (Information on the Payer) Regulations 2017, S.I. 2017/692 regulation 8(2). Hereinafter 'MLRs'.
[80] The term is defined as 'a firm or sole trader who by way of business trades in goods … when the trader makes or receives, in respect of any transaction, a payment or payments in cash of at least 10,000 euros in total'. Ibid, Regulation 14.
[81] Nicholas Ryder, Samantha Bourton, Henry Hillman and Demelza Hall, 'Higher Education Institutions and Money Laundering' (Wales Fraud Forum Annual Conference, Cardiff, September 2022).

not restricted in practice to financial or credit institutions. s.339ZB of POCA should also be applied to the entirety of the regulated sector, or, a clause similar to s.339ZD of POCA could be added to the Bill, to facilitate the disclosure of Super SARs.

- HMG must reconsider creating a single Economic Crime Agency.[82] The ECA would be responsible for all areas of financial crime, and it would gain these areas of responsibility from other existing agencies,.[83] As demonstrated above, the existing exchange of information model has become unworkable with conflicting priorities, overlapping roles and ineffective outcomes. The ECA should be managed by the Home Office, with the hope of ending the UK's 'piecemeal' approach towards the exchange of information.[84] On a grand scale, proposals for introducing the ECA could be revisited, for creating a central agency tasked with investigating all financial crimes would necessarily reduce the need for information exchange between a plethora of LEAs. Additionally, or alternatively, HMRC's experience with the automatic exchange of information suggests that automatic access to financial intelligence may also be useful for other LEAs. In this respect, it is disappointing that the Home Office cancelled plans to build a bank account portal, which would have provided LEAs with near automatic access to bank account ownership information.[85] Indeed, the benefits of providing LEAs with their own access to important financial intelligence is also demonstrated by the gains that accrued to LEAs after they gained direct access to the SAR database. One of the main reasons for the failure to build the bank account portal was the threat presented by increased compliance costs.[86] On a smaller scale, minor reforms could be made to the legal frameworks pertaining to money laundering, fraud, and tax evasion to facilitate the exchange of information between national LEAs.

- The reporting of fraud could become mandatory.[87] There are advantages to adopting this approach – it will lead to an enhanced understanding of fraud, and result in better intelligence for policing fraud. It is interesting to note that Actions 10 (the promotion

[82] HM Government, *The Coalition: Our Programme for Government* (HM Government 2010) 9. Hereinafter 'ECA'.
[83] ibid.
[84] Home Office, 'Home Office to Take Lead on Economic Crime' (January 17 2011) available from <http://www.homeoffice.gov.uk/media-centre/news/economic-crime> accessed January 11 2022.
[85] The Law Society, 'Plans to Build Bank Account Portal Cancelled' (August 12 2021) available from <https://www.lawsociety.org.uk/topics/anti-money-laundering/plans-to-build-bank-account-portal-cancelled> accessed August 12 2022.
[86] ibid.
[87] See Goldstraw-White, J. and Gill, M. The mandatory reporting of fraud: Finding solutions and sharing best practice (Fraud Advisory Panel: 2021) at 39-41.

of information sharing in relation to fraud) and 26 (strengthening the reporting of fraud) of HMG's Economic Crime Plan have yet to be addressed by HMG.[88]

- However, if fraud reporting does become mandatory, it will lead to an increased financial burden on reporting entities. HM Treasury announced that it would initially provide £18m, followed by an additional £12mto tackle money laundering and fraud.[89] This funding is supported by the Economic Crime Levy,[90] which contributes £100 million per year.[91] However, the impact of the Economic Crime Levy is questionable because there is no specific reference towards tackling fraud. Furthermore, the impact of the additional funding on tackling fraud has been questioned by Spotlight on Corruption which asserted that HMG only spends 0.042% of GDP, or £852 million, on tackling financial crime.[92] The All-Party Parliamentary Groups on Fair Business and Anti-Corruption and Responsible Tax concluded, 'LEAs are outspent and outgunned by criminals and the corrupt'.[93] HMG responded and stated 'we recognise the need for increased spending to tackle economic crime … [we] have developed a sustainable funding model that demonstrates our commitment to tackling economic crime'.[94] However, the amount of money equates to 0.2% of the extent of fraud, £190bn.[95]

- There are a number of mechanisms that could be introduced alongside the obligation to report fraud to soften the financial burden. Firstly, HM Treasury and the Home Office could resource and equip LEAs to tackle fraud by providing an additional £300 million.[96] Secondly, the additional funding could form part of a cross-governmental Economic Crime Fighting Fund. Thirdly, a proportion of the financial crime penalties

---

[88] See RUSI 'Economic Crime Plan Online Tracker', n/d, available from <https://rusi.org/ecp>.
[89] HM Treasury, *Autumn Budget and Spending Review 2001: A Stronger Economy for the British People* (HM Treasury 2021) 51.
[90] Economic Crime (Anti-Money Laundering) Levy Regulations 2022, SI. 2022/26.
[91] The Economic Crime Levey is paid by reporting entitles who are subjected to the AML/CTF reporting obligations. See HM Revenue & Customs 'Policy paper – Economic Crime (Anti-Money Laundering) Levy', (October 27 2021) available from <https://www.gov.uk/government/publications/economic-crime-anti-money-laundering-levy/economic-crime-anti-money-laundering-levy> accessed July 7 2022.
[92] All Parliamentary Group on Anti-Corruption and Responsible Tax *Economic Crime Manifesto* (All Parliamentary Group on Anti-Corruption and Responsible Tax 2022)
[93] Ibid.
[94] Ibid.
[95] National Crime Agency 'Fraud', n/d, available from https://www.nationalcrimeagency.gov.uk/what-we do/crime-threats/fraud-and-economic-crime, accessed May 1 2020. Also see National Audit Office *Progress Combatting Fraud* (National Audit Office 2022) and House of Lords Fraud Act 2006 and Digital Fraud Committee *Fighting Fraud: Breaking the Chain* HL Paper 87 Report of Session 2022–23 (House of Lords 2022).
[96] See above, n 92.

received by the FCA should be redistributed from HM Treasury, who receive the fines in excess of enforcement costs, towards supporting the mandatory reporting of fraud.

- Minor amendments could also be made to the legal framework to improve the exchange of information in tax cases, between HMRC and other LEAs. In this respect, the CRCA 2005 should be amended to require, rather than permit, disclosure when HMRC employees suspect, or have reasonable grounds to suspect, that they are in possession of information that reveals indications of money laundering or terrorism. This would be similar to the obligation to report SARs under the POCA 2002 and TACT. Alternatively, or in addition to, amendment of s.18, information exchange would be facilitated by the incorporation of an additional statutory function for HMRC in s.5 of the CRCA. In addition to HMRC's primary function of revenue collection, HMRC should be tasked with a subsidiary function of preventing and detecting tax crimes and other financial crimes encountered in the course of its primary revenue collection function.

November 2022