Export Controls, Sanctions, and Financial Intelligence: Comparing the Legal Frameworks for the Enforcement Role of Banks in the United Kingdom with Switzerland

Francesco Gaetano Fazzi*

I. Introduction

Despite the growing dominance of national security concerns in the United Kingdom ("UK"), rulings by executive and judicial authorities relating to intelligence-related national security law remain underexplored in legal literature.[1] This article addresses a specific gap in national security law literature by examining the role of financial intelligence ("FININT") in the enforcement of export controls and sanctions in the UK with a focus on secondary legislation and case law. The use of FININT to detect potential violations of export controls and sanctions has received limited scholarly attention,[2] not only in the context of sanctions against Russia, despite its growing significance to the UK due to current geopolitical risks. Among the few related articles, those written by legal scholars are particularly scarce.

* King's College London, Dickson Poon School of Law. The author holds a Master of Laws (LL.M.), Peking University, School of Transnational Law (2025); Diploma of Advanced Studies in Law & Management, University of St. Gallen (2023); MBA, University of Oxford, Saïd Business School (2020); Master in Public Policy, National University of Singapore, Lee Kuan Yew School of Public Policy (2019); Bachelor of Science in Chemistry, University of Zurich (2017). Most of this article was written in residence during the 2025 International Security and Intelligence Programme at the University of Cambridge, organized by the Cambridge Security Initiative and King's College London. The author would like to express his gratitude to Emmanuel College for its hospitality during residence. Further, the author would like to thank the researchers at the Royal United Services Institute for their outstanding work and the *Journal of National Security Law & Policy* Editorial Team for their great support in getting this article published.

1. Robert Ward, *National Security, Intelligence, and the Law*, *in* National Security Law, Procedure and Practice 3, ¶¶ 1.01–1.02 (2d ed. Robert Ward et al. eds., 2023).

2. For related publications, see Olivia Allison & Tom Keatinge, *Strengthening the Financial Frontline on Russian Trade Sanctions*, Royal United Servs. Inst. (Mar. 3, 2025), https://perma.cc/HRT6-6ZCB; Benjamin Hilgenstock, Elina Ribakova, Anna Vlasyuk & Guntram Wolff, *Enforcing Export Controls Learning from and Using the Financial System*, 16 Glob. Pol'y 190 (2025); Michael E. Zolandz & Shahrzad Noorbaloochi, *Russia Sanctions and Circumvention: Fortifying Global Due Diligence and Screening in the Face of Evolving Schemes*, 8 J. Fin. Compliance 389 (2024); Louis de Koker, *The FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges*, *in* Financial Crime and the Law: Identifying and Mitigating Risks 123 (Doron Goldbarsht & Louis de Koker eds., 2024); Shacheng Wang, Xixi Zhu & Bing Zhang, *A New Financial Crime: Proliferation Financing and China's Countermeasures*, 36 Sec. J. 272 (2023); Ian John Stewart, Andrea Viski & Jonathan Brewer, *Combating the Financing of Proliferation: Challenges and New Tools*, 27 J. Fin. Crime 1107 (2020); Rachel A. Weise, Gretchen Hund & Geoffrey Carr, *Export Controls and Counterproliferation Finance: Two Sides of the Same Underlying Illegal WMD Activity*, 25 Nonproliferation Rev. 129 (2018); Moyara Ruehsen & Leonard Spector, *Follow the Proliferation Money*, 71 Bull. Atomic Scientists 51 (2015).

This article not only contributes to closing the gap in legal literature but also does so with a novel approach. First, while existing publications focus on reporting obligations under anti-money laundering ("AML") and countering the financing of terrorism ("CFT") legislation that generates FININT, this article also examines the overlooked reporting obligations under export control and sanctions legislation. Second, since export controls and sanctions are predominant topics in contemporary international economic law,[3] this article takes public international law as the starting point, thereby underscoring that all United Nations ("UN") member states have a legally binding obligation to establish a legal framework for their financial institutions to generate FININT in the form of suspicious activity reports ("SARs").

Third, the article compares the reporting obligations for banks under export control, sanctions, and AML/CFT legislation between the UK and Switzerland in the context of their increasing collaboration in financial and national security matters post-Brexit with binding and non-binding instruments of public international law and comparable risk exposure to proliferation financing ("PF").

In light of a novel mutual recognition agreement between both countries, under which each jurisdiction recognizes specified areas of the other's financial services regulatory and supervisory framework as equivalent, this article aims to answer the question of whether the reporting obligations for banks for suspected violations of export controls and sanctions under UK export control, sanctions, and AML/CFT legislation are equivalent to those under Swiss law.[4]

The article argues that these reporting obligations are not equivalent. Specifically, it contends that the UK, unlike Switzerland, has addressed a legislative gap by introducing a reporting obligation for banks concerning suspected violations of trade sanctions, thereby creating an additional valuable and effective source of FININT for the UK government. Nevertheless, as in Switzerland, the absence of a corresponding reporting obligation under export control legislation means that FININT for suspected violations in this area continues to rely on reporting under the AML/CFT framework, which in practice remain prone to inefficiencies.

This article is divided into four parts. The first part explores post-Brexit collaboration between the UK and Switzerland in the financial services and security sectors, with a particular focus on their PF risks and the role of FININT, especially SARs. The second part analyzes reporting obligations under the UK's export control and sanctions legislation. The third part examines reporting obligations under the UK's AML/CFT framework, comparing these obligations to the corresponding Swiss requirements, and highlights practical challenges in

3. Joel Slawotsky, *Conceptualizing National Security in an Era of Transformative Technologies and Strategic Conflict*, *in* A RESEARCH AGENDA FOR GLOBAL POWER SHIFTS AND INTERNATIONAL ECONOMIC LAW 147 (Joel Slawotsky ed., 2025).

4. For a previous, outdated comparison of the UK AML/CFT framework with the Swiss framework, see Igho L. Dabor, *Crying Wolf: An Examination of the UK's Suspicious Activity Report Regime*, 40 CO. LAW. 107 (2019).

enforcement. The final part addresses these practical challenges and ends with a final comparison between the UK and Swiss reporting obligations for banks.

The information in this article is current as of September 1, 2025, when the writing was completed.

II. UK–SWITZERLANDCOOPERATION, PROLIFERATION FINANCING RISKS, AND FINANCIAL INTELLIGENCE

A. Growing Collaboration Between the United Kingdom and Switzerland in Financial Services and Security

The UK and Switzerland are forging closer ties. On December 21, 2023, both countries signed an agreement on mutual recognition in financial services: the Berne Financial Services Agreement ("BFSA").[5] The BFSA aims to improve the competitiveness and enhance cooperation between the two international financial centers.[6] It is a bilateral and reciprocal enhancement of the liberalization in financial services trade established based on Article VII of the General Agreement on Trade in Services ("GATS").[7] GATS entered into force on January 1, 1995, and both the UK and Switzerland are Contracting States to it.[8]

The BFSA is unique, as for the first time, two states have mutually recognized the equivalence of their respective legal and supervisory frameworks in certain areas of the financial services sector.[9] This will allow qualified financial services providers to provide certain services from their respective home state to certain clients in the host state without requiring additional licensing from the host state.[10] *Inter alia*, this includes the provision of cross-border banking services.[11] The providers will remain under the supervision of the financial regulator and subject to the legislation of their home state,[12] including AML, CFT, export control, and sanctions legislation. The Agreement is expected to enter into force in early 2026.[13]

---

5. *Switzerland and the UK Sign Agreement on Mutual Recognition in Financial Services*, STATE SECRETARIAT FOR INT'L FIN. MATTERS (Dec. 21, 2023), https://perma.cc/K4M5-44J8. *See* Agreement Between the United Kingdom of Great Britain and Northern Ireland and the Swiss Confederation on Mutual Recognition in Financial Services, Switz.-UK, Dec. 21, 2023, https://perma.cc/GSK9-TUFL [hereinafter Berne Financial Services Agreement].

6. STATE SECRETARIAT FOR INT'L FIN. MATTERS, *supra* note 5.

7. Jonathan R.M. Foster, *The Magnificent Seven: Exemption, Relief, Equivalence, Recognition, Substitution, Deference, Trust – Reducing Regulatory Duplication and Frictions in the Cross-Border Supply of Financial Services*, 15 EUR. J. RISK REGUL. 33, 44; General Agreement on Trade in Services art. VII, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167.

8. *Marrakesh Agreement Establishing the World Trade Organization*, U.N. TREATY COLLECTION, https://perma.cc/R7VJ-WZPW.

9. STATE SECRETARIAT FOR INT'L FIN. MATTERS, *supra* note 5.

10. *Id.*

11. *Id.; see also* Foster, *supra* note 7, at 39 (noting that "[t]he effect is that compliance with the other jurisdiction's regime is substituted for compliance for its own, so that a [financial services] supplier need comply only with the rules of a single (home state) regulatory regime").

12. STATE SECRETARIAT FOR INT'L FIN. MATTERS, *supra* note 5.

13. *Berne Financial Services Agreement for UK and Swiss Firms*, FIN. CONDUCT AUTH. (July 23, 2025), https://perma.cc/UL8F-VUSW.

Similarly, Switzerland has expressed its intention in June 2025 to adopt a "senior managers regime" for banks,[14] an innovative regulation first introduced in the UK in 2016 to "address a deficit in public trust in banks and bankers."[15] This regime aims to prevent misconduct by requiring Swiss financial institutions to clearly define individual management responsibilities,[16] including AML/CFT responsibilities. Misconduct can then be clearly attributed, enabling targeted regulatory sanctions such as claw-backs, bonus reductions, or professional bans imposed by the Swiss financial regulator.[17]

Given both the UK and Switzerland's similarities in the global economic order, their ambition for closer collaboration is understandable. London ranks as the second top financial center globally, while Geneva and Zurich rank among the top ten in Western Europe.[18] Simultaneously, the UK and Switzerland are ranked among the top five most innovative countries (fifth and first, respectively),[19] and are thus incubators for technology that can be used for civilian and military purposes (dual-use technology). While Switzerland has never been a member of the European Union ("EU"), the UK famously left the EU in 2020, leaving both states among the minority of non-EU states in Europe.

Conversely, their position in the global security order is vastly different. The UK is a Contracting State to the North Atlantic Treaty Organization ("NATO") and Five Eyes Alliance, a permanent member of the UN Security Council ("UNSC"), and one of the world's five official nuclear powers. Switzerland, on the other hand, is none of these.[20]

Despite its neutrality, Russia's invasion of Ukraine has not left Switzerland's national security and foreign policy untouched. In response to the invasion, Switzerland decided in February 2022 to adopt the EU's sanctions against Russia.[21] Although it clarified in a press conference in September 2022 that this

14. Press Release, Swiss Fed. Dep't of Defence, Civil Protection & Sport, Federal Council Draws Lessons from Credit Suisse Crisis and Defines Measures for Banking Stability (June 6, 2025), https://perma.cc/P4Y5-5G2A [hereinafter Federal Council Press Release].

15. Eleanore Hickman & Alan Brener, *The Senior Managers and Certification Regime in UK Practice and Global Context*, 26 J. BANKING REGULS. 356, 356 (2025). This follows a global trend, as similar regimes have been introduced in some common law jurisdictions like Ireland, Australia, Singapore, Malaysia, and Hong Kong. *Id.* at 363–65.

16. Federal Council Press Release, *supra* note 14.

17. *Id.*

18. Z/YEN & CHINA DEV. INST., THE GLOBAL FINANCIAL CENTRES INDEX 37 22 (2025), https://perma.cc/8MSY-W62H.

19. WORLD INTELL. PROP. ORG., GLOBAL INNOVATION INDEX 2024: UNLOCKING THE PROMISE OF SOCIAL ENTREPRENEURSHIP 18 (17th ed. Soumitra Dutta, Bruno Lanvin, Lorena Rivera León & Sacha Wunsch-Vincent eds., 2024), https://perma.cc/XZ5M-HKWU.

20. Switzerland's atomic bomb program never came to fruition. *See* Michael Fischer, *The Swiss Atomic Bomb*, SCHWEIZERISCHES NAT'L MUSEUM BLOG (last updated July 15, 2022), https://perma.cc/C4AN-UD8K. According to Privacy International, the Five Eyes have a "focused cooperation" with Switzerland. *See* Carly Nyst, *The Five Eyes Fact Sheet*, PRIV. INT'L (Nov. 26, 2013), https://perma.cc/UFV9-VMCG.

21. *Switzerland Adopts EU Sanctions Against Russia*, FED. COUNCIL (Feb. 28, 2022), https://perma.cc/Y64M-UPKX.

unprecedented step does not signify a deviation from its long-standing neutrality policy,[22] subsequent decisions seem to tell a different story. In April 2023, the UK and Switzerland signed a non-binding declaration of intent to formalize future security dialogues.[23] The agreement identifies potential areas of collaboration between the two countries, including military training and cooperation in the technology sector.[24]

In January 2024, Switzerland announced that its "security and defence policy will be geared more consistently to international cooperation, especially with NATO, the EU and neighbouring countries,"[25] a move supported by the Swiss public.[26] In October 2024, Switzerland signed the declaration to join the European Sky Shield Initiative ("ESSI"), a project aiming to build an air and missile defense system across Europe.[27] The UK, in contrast, already signed such a declaration to join the ESSI in October 2022.[28]

In law enforcement, the UK and Switzerland signed a Police Cooperation Agreement in December 2020, prior to Russia's invasion of Ukraine, building upon a Memorandum of Understanding from July 2019, to "facilitate the exchange of information and intelligence in order to assist investigations and tackle crime."[29] It commits both countries to "undertake a range of activity together to strengthen joint capacity to combat crime, terrorism and corruption."[30] Like the BFSA, the Agreement forms part of a broader set of bilateral agreements established following the UK's departure from the EU, aimed at preserving and deepening the strong ties between the UK and Switzerland after the transition period.[31]

The Police Cooperation Agreement aims to enhance cooperation, *inter alia*, in the areas of economic and financial crime, including ML, and trafficking in

---

22. *Questions and Answers on Switzerland's Neutrality*, FED. DEP'T OF FOREIGN AFFS. (Sept. 9, 2022), https://perma.cc/PXF9-PRPD.

23. *Switzerland and UK Conclude Security Partnership*, SWISSINFO (Apr. 20, 2023), https://perma.cc/K9R2-UEJN.

24. *Id.*

25. *Federal Council Approves Report on Strengthening the Defence Capability of the Armed Forces and Deepening International Cooperation*, FED. COUNCIL (Jan. 31, 2024), https://perma.cc/MEQ9-VRLX. *See also Relations with Switzerland*, N. ATL. TREATY ORG. (last updated May 2, 2025), https://perma.cc/BK34-ESHE; *Switzerland Steps Up Defence Cooperation with NATO*, SWISSINFO (Mar. 21, 2025), https://perma.cc/MRX5-37DR; Thomas Stephens, *Switzerland and NATO: Just Flirting or the Start of a Wild Marriage?*, SWISSINFO (Feb. 2, 2024), https://perma.cc/HN2T-NTZG; Katy Romy, *Switzerland Mulls Stronger Ties with European Defence Structures*, SWISSINFO (June 9, 2025), https://perma.cc/RW77-P48U.

26. *The Swiss Want More Cooperation with NATO*, SWISSINFO (June 18, 2025), https://perma.cc/2ASH-AKCW.

27. *Neutral Switzerland Signs Declaration to Join European Sky Shield Initiative*, REUTERS (Oct. 18, 2024), https://perma.cc/28H3-5UTY.

28. CLAIRE MILLS, HOUSE OF COMMONS LIBR., UK DEFENCE IN 2025: INTEGRATED AIR AND MISSILE DEFENCE 14 (2025), https://perma.cc/LL9A-K2ER; *14 NATO Allies and Finland agree to boost European air defence capabilities*, N. ATL. TREATY ORG. (Oct. 23, 2022), https://perma.cc/9M96-6XSX.

29. U.K. Home Off. & Rt. Hon. James Brokenshire, *UK and Switzerland Sign New Police Co-operation Agreement*, GOV.UK (Dec. 15, 2020), https://perma.cc/6R6A-5N43.

30. *Id.*

31. *Id.*

weapons, explosives, and their precursors.[32] Correspondingly, it facilitates the exchange of information on legislative and scientific tools used to combat crime, including analysis of criminal and terrorist threats, and covers the sharing of intelligence and analytical data related to terrorism and serious crime.[33] Additionally, the Agreement enables the exchange of information on economic and financial crimes such as ML, including via the tracing of assets of criminal origin, as well as on illegal activities involving weapons and explosives.[34] The wide scope of the Agreement underscores its potential to enhance the enforcement of export controls and sanctions in both countries through collaboration and intelligence sharing.[35]

While the UK and Switzerland have not conducted an exercise to determine the equivalence of their sanction regimes against Russia, the EU has done just that, albeit from its own perspective. Under Annex VIII of Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, the legal basis for the EU's sanctions against Russia, both the UK and Switzerland are considered "partner countries."[36] However, unlike Switzerland, the UK has adopted its own sanctions regime against Russia rather than according it to the EU's sanctions.

B. Growing Proliferation Financing Risk

Financial institutions play a vital role in enforcing export controls and sanctions.[37] In June 2025, the Financial Action Task Force ("FATF") published its first-ever dedicated typologies report focused specifically on complex PF and sanctions evasion schemes.[38] The FATF is considered "the single most important international body in terms of formulating antimoney-laundering policy and developing international standards for disclosure and transparency for financial institutions."[39] While both the UK and Switzerland are members of the FATF, Russia's membership was suspended in February 2023 in response to its invasion of Ukraine.[40] The FATF defines PF as follows:

32. Agreement on Police Cooperation arts. 4(2)(a), (g), (m), U.K.-Switz., Dec. 15, 2020, TS No. 2/2022, CP 580.

33. *Id.* arts. 5(1)(a)(v), (viii).

34. *Id.* arts. 5(1)(a)(ix)–(x).

35. While the Agreement mentions the Federal Office of Police in Switzerland as a "competent authority," which is home to the Swiss Financial Intelligence Unit, it does not mention the State Secretariat for Economic Affairs ("SECO"), which enforces export controls and sanctions in Switzerland. *Id.* art. 3(1)(b)(i); Francesco Gaetano Fazzi, *The Role of Financial Institutions in Enforcing Export Restrictions in Switzerland*, 34 J. FIN. REGUL. & COMPLIANCE 100, 102 (2026). *See also* notes 42, 155, 176.

36. Council Regulation 833/2014, Annex VIII, 2014 O.J. (L 229) 1 (EU).

37. *See* note 2.

38. FIN. ACTION TASK FORCE, FATF REPORT: COMPLEX PROLIFERATION FINANCING AND SANCTIONS EVASION SCHEMES (2025), https://perma.cc/L8ZL-FYFV.

39. KERN ALEXANDER, RAHUL DHUMALE & JOHN EATWELL, GLOBAL GOVERNANCE OF FINANCIAL SYSTEMS: THE INTERNATIONAL REGULATION OF SYSTEMIC RISK 150 (2005).

40. *FATF Statement on the Russian Federation*, FIN. ACTION TASK FORCE (Feb. 24, 2023), https://perma.cc/9VH6-ERQX.

> Raising, moving, or making available funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of [weapons of mass destruction ("WMD")] proliferation, including the proliferation of their means of delivery and related materials (including dual-use technologies and dual-use goods for non-legitimate purposes).[41]

Sanctions evasion and PF have been recognized by the UK as a major risk. Sanctions evasion facilitated by UK-based or UK-registered "professional enablers," particularly linked to the Russian invasion of Ukraine, appeared on top of the National Crime Agency's ("NCA"), the UK's Financial Intelligence Unit ("FIU"),[42] System Priorities on July 21, 2025, with full endorsement of the UK's financial regulator, the Financial Conduct Authority ("FCA").[43] Similarly, both the Swiss FIU and the Swiss financial regulator have retroactively declared trade-based sanctions as the priority risk for 2024.[44]

For Switzerland, the risk does not only stem from Swiss sanctions against Russia,[45] but also from being used as an intermediary country,[46] for instance, to process funds of UK-sanctioned individuals.[47] This is evident from a recent case in the United States. In December 2024, two individuals were charged by a federal court in the United States with "conspiring to export U.S.-origin electronics to an Iran-based supplier of the Islamic Revolutionary Guard Corps."[48] One of the charged Iranian nationals completed post-doctoral work at the Ecole Polytechnique Federale de Lausanne, a leading Swiss research university, where he evaded export controls on Iran by repeatedly shipping electronic components of U.S. origin through his university address to Iran.[49] In September 2019, he went a step further and created a Swiss company jointly with another Iranian national and Swiss resident, which was used as a front to evade U.S. export controls.[50] These parts were later used in drones

41. FIN. ACTION TASK FORCE, *supra* note 38, at 8 (noting that there is no universal definition of WMD proliferation or PF).

42. Like HMRC, the NCA is a "competent authority" under the Agreement on Police Cooperation between the UK and Switzerland. Agreement on Police Cooperation, *supra* note 32, art. 3(1)(a)(iii).

43. NAT'L CRIME AGENCY, SYSTEM PRIORITIES – 2025 1–3 (2025), https://perma.cc/8H6R-K5MT.

44. Fazzi, *supra* note 35, at 103.

45. *Id.*

46. The Office of Financial Sanctions Implementation ("OFSI") highlighted in a February 2025 report that "since February 2022, just over 25% of suspected breach reports received by OFSI from UK financial services firms have made reference to intermediary jurisdictions. The following jurisdictions feature most often: British Virgin Islands (BVI); the Republic of Cyprus; Switzerland; United Arab Emirates (UAE); Guernsey; Luxembourg; Austria; and Türkiye." OFF. OF FIN. SANCTIONS IMPLEMENTATION, HM TREASURY, FINANCIAL SERVICES THREAT ASSESSMENT 24 (2025), https://perma.cc/7ABU-CUZE (further stating that "[i]t should be noted that a reference to an intermediary jurisdiction in a report of a suspected sanctions breach does not necessarily mean that any sanctions breach has occurred in that jurisdiction, or that the jurisdiction does not enforce sanctions effectively").

47. *Id.* at 25.

48. Paul Esau, *U.S. Disrupts Iranian Procurement Scheme Tied to Drone Attacks on U.S. Military Base*, IRAN WATCH (Apr. 16, 2025), https://perma.cc/Y3AV-CJUP.

49. *Id.*

50. *Id.*

that attacked U.S. military facilities.[51] In September 2023, Switzerland enhanced its sanctions against Iran by prohibiting the sale, delivery, export and transit of components used for the construction and production of drones, albeit in the context of the EU's sanctions against Russia.[52]

Combating PF is arguably the least known out of the FATF's three defined mandates, which also comprise the better-known mandates of AML and CFT.[53] Although FATF's recommendations, on their own, are not legally binding, the UNSC has rendered their implementation legally binding to UN member states. The first UNSC resolution ("UNSCR") to refer to the FATF Recommendations was UNSCR 1617 in 2005.[54] UNSCR 1617 "strongly urges" UN member states to "implement the comprehensive, international standards embodied in the [FATF] Forty Recommendations on Money Laundering and the FATF Nine Special Recommendations on Terrorist Financing."[55]

This call for action was repeated in UNSCR 2462 of 2019, notably in the same year of the FATF's 30th anniversary, as the resolution "strongly urges" UN member states to implement *all* FATF Recommendations,[56] including its recommendations on PF. Just a year prior, the FATF published its guidance on counter PF.[57] The FATF's mandate, though, only applies to combat the financing of WMD by non-state actors as well as the Democratic Republic of Korea ("DPRK") based on the respective UNSCRs.[58]

Since UNSCR 2462, the world has undergone significant geopolitical changes. The UNSC has lifted its sanctions against Iran in October 2023,[59] leaving the DPRK the single state against which UN sanctions still exist, notably since 2006, due to its WMD program.[60] In June 2024, Russia signed a Comprehensive Strategic Partnership Treaty with the DPRK, which entered into force in December 2024 and includes the provision of military assistance and joint measures to bolster defense capabilities and was accompanied by a deployment of

51. *Id.*

52. *Ukraine: Switzerland Adopts EU Sanctions Against Iranian Drone Industry*, SWISSINFO (Sept. 29, 2023), https://perma.cc/TM7R-FGMC.

53. *Mandate of the Financial Action Task Force*, FIN. ACTION TASK FORCE (Apr. 12, 2019), https://perma.cc/EF9U-78LU.

54. Cheong-Ann Png, *International Legal Sources II—The United Nations Security Council Resolutions*, *in* BANKS AND FINANCIAL CRIME: THE INTERNATIONAL LAW OF TAINTED MONEY 39 (2nd ed. William Blair, Richard Brent & Tom Grant eds., 2017).

55. S.C. Res. 1617, ¶ 7, U.N. Doc. S/RES/1617 (July 29, 2005).

56. S.C. Res. 2462, ¶ 4, U.N. Doc. S/RES/2462 (Mar. 9, 2019); *see also* William Casey King & Richard Gordon, *United Nations Security Council Resolution 2462*, 59 INT'L LEGAL MATERIAL 252, 253 (2020).

57. *See generally* FIN. ACTION TASK FORCE, GUIDANCE ON COUNTER PROLIFERATION FINANCING: THE IMPLEMENTATION OF FINANCIAL PROVISIONS OF UNITED NATIONS SECURITY COUNCIL RESOLUTIONS TO COUNTER THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (2018), https://perma.cc/TV4A-RY8A.

58. *Id.* at 3–4.

59. FIN. ACTION TASK FORCE, *supra* note 38, at 15.

60. *Id.* at 12.

DPRK soldiers in the ongoing Russia-Ukraine conflict,[61] thereby effectively extending the PF risk relating to DPRK to Russia.

It is important to note, though, that the scope of PF under the FATF is not congruent with sanctions or export controls.[62] PF is conceptually analogous to CFT, insofar as both regimes address the provision and use of funds or financial services, including transactions, in support of prohibited activities. However, under the FATF Recommendations, PF is reflected in the implementation of financial sanctions imposed by the UNSC,[63] which, in any case, are already legally binding on UN member states,[64] while the broader concept of PF extends beyond these sanctions and may be addressed through additional national measures, including sanctions and export control legislation that go beyond the requirements of UNSCRs.

In practice, this means that an export license may have been granted for dual-use goods for the export to a third state for a legitimate purpose. However, from that third state, the goods may then be re-exported to the DPRK. Whether the export license has been obtained under false pretenses becomes an issue of export controls, while the evasion of sanctions and the use of financial institutions and their services for that purpose most likely fall under sanctions and ML, depending on the jurisdiction.[65]

In their 2018 publication, one of the few scholarly publications on the role of financial institutions in enforcing export controls and sanctions but written from the U.S. perspective, Rachel A. Weise, Gretchen Hund and Geoffrey Carr elaborate on the scope of PF. They argue that combating PF is

> broader than simply refusing to do business with entities on UN sanctions lists or maintaining lists of export-controlled commodities (relatively easy tasks); it also requires identifying suspicious activities and financial transactions that support proliferation (a relatively difficult task). Entities that are not sanctioned may be involved in illicit acquisitions, frequently involving dual-use goods. Linking an attempt to procure sensitive items with non-sanctioned entities seeking to acquire those items is challenging, and has received far less attention than it warrants.[66]

According to the FATF, "the most significant PF threat to the international financial system is posed by state-sponsored or -affiliated actors, including but not limited to those associated with sanctions evasion and PF activities related to the DPRK."[67] International financial centers are at risk of PF and sanctions evasion

61. *Id.* at 13, 15–16; *North Korea-Russia treaty comes into force, KCNA says*, REUTERS (Dec. 4, 2024), https://perma.cc/657D-GP2N; *Law on ratification of Russia-DPRK comprehensive strategic partnership treaty*, KREMLIN (Nov. 9, 2024), https://perma.cc/DY94-3P9H.

62. *See* Fazzi, *supra* note 35, at 101 (on the difference between sanctions and export controls).

63. de Koker, *supra* note 2, at 130–31.

64. Weise, Hund & Carr, *supra* note 2, at 134.

65. *See* Stewart, Viski & Brewer, *supra* note 2, at 1112 (noting that the U.S. does not recognize PF as a stand-alone offense and has prosecuted PF-related cases under sanctions, export controls, and ML).

66. Weise, Hund & Carr, *supra* note 2, at 130.

67. FIN. ACTION TASK FORCE, *supra* note 38, at 11 (acknowledging the importance of a broader concept of PF, while simultaneously highlighting that "PF risk refers strictly and only to the potential

due to their "importance to global financial flows and transport,"[68] which puts the UK, with the second most important financial center globally, in the scope of PF and sanction evasion prevention. Simultaneously, the UK is the world's second leading shipping center.[69] Conversely, Switzerland has become the world's largest shipping container nation, despite being landlocked,[70] which imposes a PF risk on banks servicing this industry.[71] Finally, innovative countries that produce proliferation-sensitive technologies and goods such as the UK and Switzerland are inherently exposed to a higher risk of PF and violations of dual-use goods restrictions.[72]

Although 61% of European banks claim to have a compliance function that incorporates PF,[73] the FATF criticizes that the global implementation of measures against PF is "still lagging" and that due to "the absence of a robust regulatory, legislative, and operational framework, some countries are not able to apply the required sanctions obligations and export controls to deter and counter proliferation networks."[74]

Against this backdrop, the author previously described how the Swiss AML/CFT legal framework complements the absence of reporting obligations for financial institutions in export control and sanctions legislation in Switzerland.[75] Given that the UK and Swiss financial markets are bound to become more closely integrated in the near future, this development warrants a comparative analysis of the UK framework with the Swiss.

C. Financial Intelligence

FININT is one in a myriad of sources for government intelligence services.[76] However, despite its effectiveness, it is underappreciated[77] and

---

breach, non-implementation, or evasion of the [financial sanctions] obligations referred in Recommendation 7, which focuses solely on that UN-sanctioned country, the DPRK").

68. *Id.* at 17.

69. *2025 Xinhua-Baltic International Shipping Center Development Index: Singapore Leads Shipping for 12th Year*, AM. J. TRANSP. (July 11, 2025), https://perma.cc/2E2A-LY9E.

70. *Landlocked Switzerland Becomes World's Largest Container Ship Nation*, SWISSINFO (Mar. 11, 2025), https://perma.cc/EFY8-6RBC.

71. FIN. ACTION TASK FORCE, *supra* note 38, at 17.

72. *Id.* at 18.

73. Based on a survey conducted in 2019 and 2020 by the Royal United Services Institute ("RUSI") and the Association of Certified Anti-Money Laundering Specialists ("ACAMS") with a sample of 366 respondents working at international, regional, and national banks across the globe. EMIL DALL & JUSTINE WALKER, ROYAL UNITED SERV. INST. & ASS'N OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS, RUSI-ACAMS PROLIFERATION FINANCE SURVEY 4 (Feb. 6, 2020), https://perma.cc/3BKV-JK7P.

74. FIN. ACTION TASK FORCE, *supra* note 38, at 17–18.

75. Fazzi, *supra* note 35, at 110.

76. Anthony Amicelle, *(Il)légitimité du renseignement financier: usages transnationaux de la traçabilité des flux de capitaux*, 47 CRIMINOLOGIE 77, 77–78 (2014). *See also* Zolandz & Noorbaloochi, *supra* note 2, at 388 (referring the use of "intelligence resources" in the United States to "trace and disrupt complex networks that it believes facilitate access to the US financial system or enable the export of restricted goods and technology to Russia").

77. Matthew Levitt, *Follow the Money: Leveraging Financial Intelligence to Combat Transnational Threats*, 12 GEO. J. INT'L AFFS. 34, 35 (2011).

underutilized.[78] Its importance was underscored in July 2006, when al-Qaeda nearly carried out what would have been its deadliest attack since 9/11.[79] A group of British citizens planned to detonate liquid explosives on at least ten airliners bound from the UK to the United States and Canada.[80] The plot was foiled by UK authorities, largely due to FININT.[81] In response, UK officials swiftly announced plans to expand the use of FININT tools to disrupt future terrorist operations.[82]

Similarly, in the aftermath of the lone-wolf terrorist attack of Anders Behring Breivik in Norway in July 2011, FININT on Breivik allowed Finnish authorities to apprehend another individual with similar terrorist intentions before they could carry out their plans.[83] FININT was furthermore critical in identifying the involvement of Iranian state-owned banks in illicit activities aiming to "secretly proliferate terrorism financing and WMD programs."[84]

On the often-overlooked value of FININT, the former Deputy National Security Advisor for combating terrorism during the George W. Bush administration, Juan Carlos Zarate, noted:

> What makes [FININT] so valuable is that it can reveal clear contours of relationships. Unlike the vagaries and complications of human intelligence (HUMINT) or misinterpreted and incomplete captured communications (SIGINT), financial footprints don't lie. The passing of cash between operatives confirms a connection; the wiring of money between banks unveils a relationship between the account holders; the transfer of money or goods between brokers identifies historical business ties. The records of those transactions—addresses, phone numbers, real names, banks utilized—can be a gold mine of information . . . Money is the great facilitator and connector—even among enemies.[85]

The origins of FININT can be traced back to the 1989 Paris Summit of the Group of Seven countries with the aim to combat ML at a global scale, which subsequently established the FATF.[86] After the 9/11 attacks in 2001, the FATF

---

78. TOM KEATINGE, ANTON MOISEIENKO, FLORENCE KEEN, DAVID ARTINGSTALL & HELENA WOOD, ROYAL UNITED SERVS. INST., NO REST FOR THE WICKED: DRIVING CHANGE IN THE UK'S POST-FATF EVALUATION AML REGIME 41–48 (2019), https://perma.cc/2F5Z-NRFW.

79. Levitt, *supra* note 77, at 34.

80. *Id.*

81. *Id.*

82. *Id.*

83. Amicelle, *supra* note 76, at 95; EUROPEAN COMM'N, COMMISSION STAFF WORKING DOCUMENT, REPORT ON THE SECOND JOINT REVIEW OF THE IMPLEMENTATION OF THE AGREEMENT BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA ON THE PROCESSING AND TRANSFER OF FINANCIAL MESSAGING DATA FROM THE EUROPEAN UNION TO THE UNITED STATES FOR THE PURPOSES OF THE TERRORIST FINANCE TRACKING PROGRAM 14–15 (Dec. 12, 2012), https://perma.cc/TG3Y-W5KB.

84. Levitt, *supra* note 77, at 36.

85. JUAN CARLOS ZARATE, TREASURY'S WAR: THE UNLEASHING OF A NEW ERA OF FINANCIAL WARFARE 48 (2013).

86. Martin Rudner, *Using Financial Intelligence Against the Funding of Terrorism*, 19 INT'L J. INTEL. & COUNTERINTELLIGENCE 32, 47 (2006).

added CFT to its mandate, which spurred the global use of FININT.[87] While the FATF already recommended in 1990 that financial institutions should be either required or permitted to inform their "competent authorities" if they suspected that funds stemmed from a criminal activity,[88] this obligation to report became legally binding to all UN member states after 9/11.[89]

Article 18(b) of the International Convention for the Suppression of the Financing of Terrorism ("Terrorist Financing Convention") requires its Contracting States to adopt their domestic legislation to obligate their financial institutions to "report transactions suspected of stemming from criminal activity."[90] Such reports are called SARs.[91]

Although the Convention had been drafted at the end of 1999, by September 2001 it had not received the necessary twenty-two ratifications to enter into force.[92] The adoption of UNSCR 1373 in response to the 9/11 attacks marked an abrupt turning point, as the UNSC called upon states to become parties to the Convention "as soon as possible."[93] The UK had already signed and ratified the Convention prior to UNSCR 1373, in January 2000 and March 2001, respectively. Switzerland, however, was slower in its adoption: while it had signed the Convention in June 2001, its ratification was in September 2003.[94]

Regarding the reporting obligation for financial institutions, the Convention accomplished two points. First, it codified the FATF's 1990 recommendation on a reporting obligation for financial institutions, initially intended to combat ML, into public international law, which became binding to all UN member states through UNSCR 1373. Second, the Convention extended the obligation's scope by requiring its Contracting States to criminalize the financing of acts of terrorism,[95] which, as a result, obligated financial institutions to also assess the intended use of funds, rather

87. *Id.*

88. FIN. ACTION TASK FORCE, THE FORTY RECOMMENDATIONS OF THE FINANCIAL ACTION TASK FORCE 4 (1990), https://perma.cc/H32Z-FPT9.

89. The FATF provides a definition of "financial institutions" in its current *Recommendations*, adopted in 2012 and updated in 2025. FIN. ACTION TASK FORCE, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION 132 (2025), https://perma.cc/U56S-AJDZ.

90. International Convention for the Suppression of the Financing of Terrorism art. 18(b), Dec. 9, 1999, 2178 U.N.T.S. 197.

91. Hussain Syed Gowhor, *The Existing Financial Intelligence Tools and Their Limitations in Early Detection of Terrorist Financing Activities*, 25 J. MONEY LAUNDERING CONTROL 843, 847 (2022). Unlike the UK, some jurisdictions use the description "suspicious transaction report" instead.

92. Ilias Bantekas, *The International Law of Terrorist Financing*, 97 AM. J. INT'L L. 315, 326 (2003).

93. S.C. Res. 1373, ¶ 3(d), U.N. Doc. S/RES/1373 (Sept. 28, 2001). UNSCR 1373 was adopted under Chapter VII of the UN Charter, thereby rendering the resolution binding. Tom Grant & Richard Brent, *General Introduction: Some Problems Relating to the Role of International Law*, *in* BANKS AND FINANCIAL CRIME: THE INTERNATIONAL LAW OF TAINTED MONEY 10 (2nd ed. William Blair, Richard Brent & Tom Grant eds., 2017) (further noting on UNSCRs 1267 and 1373 that "[t]he extent to what they bind, and precisely what they oblige their addressees to do or refrain from doing, depends on their proper construction with a view to establishing the intentions of the Security Council").

94. *11. International Convention for the Suppression of the Financing of Terrorism*, U.N. TREATY COLLECTION, https://perma.cc/U3JD-EKCQ.

95. International Convention for the Suppression of the Financing of Terrorism, *supra* note 90, art. 2.

than just their origin. This marked the beginning of the obligation's scope for both AML *and* CFT.

Although UNSCR 1373 and the Terrorist Financing Convention were not the only instruments of public international law to establish obligations for financial institutions, they should be regarded as the most significant due to the binding nature of the UNSCRs. After the Terrorist Financing Convention, the UN Convention Against Transnational Organized Crime ("Palermo Convention") obligated its Contracting States to

> institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions.[96]

The UK and Switzerland ratified the Palermo Convention in 2006.[97] Therefore, the obligations under Terrorist Financing Convention and UNSCR 1373 predated the obligations under the Palermo Convention by almost five years. While the obligations for financial institutions are arguably less fleshed out than in the Terrorist Financing Convention, the Palermo Convention is significant due to its obligation for Contracting States to criminalize ML.[98]

ML is an offense that occurs after a primary offense (i.e., the "predicate offense" under the Palermo Convention or the "criminal activity" under the Terrorist Financing Convention) from which funds have been generated. The Palermo Convention obligates Contracting States to establish "the widest range of predicate offenses,"[99] which

---

96. United Nations Convention Against Transnational Organized Crime art. 7(1)(a), Nov. 15, 2000, 2225 U.N.T.S. 209.

97. *12. United Nations Convention Against Transnational Organized Crime*, U.N. TREATY COLLECTION, https://perma.cc/GKK4-7AKP. As of August 31, 2025, only Papua New Guinea, Solomon Islands, and Tuvalu were not Contracting States to the Palermo Convention. The latest state to ratify the Convention was the Islamic Republic of Iran on August 6, 2025. *Id.*

98. United Nations Convention Against Transnational Organized Crime, *supra* note 96, art. 6(1). However, criminalizing ML was already an obligation for Contracting States under the Vienna Convention, albeit only for drug-related predicate offenses. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances arts. 3(1)(b)–(c), Dec. 20, 1988, 1582 U.N.T.S. 95. While the UK had ratified the Vienna Convention in 1991, Switzerland ratified the Convention as late as in 2005, more than thirteen months before ratifying the Palermo Convention. *19. United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, U.N. TREATY COLLECTION, https://perma.cc/JNJ8-MDYM. Moreover, prior to the Palermo Convention, the UK and Switzerland were already Contracting States to the Strasbourg Convention of the Council of Europe, which, analogous to the Palermo Convention, criminalizes ML for undefined predicate offenses. Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime arts. 1(e), 6, Nov. 8, 1990, E.T.S. No. 141. The UK and Switzerland ratified the Strasbourg Convention in 1992 and 1993, respectively. *Chart of Signatures and Ratifications of Treaty 141*, COUNCIL OF EUR., https://perma.cc/94SC-K3AW.

99. United Nations Convention Against Transnational Organized Crime, *supra* note 96, art. 6(2)(a).

has a direct effect on reporting obligations under AML/CFT legislation, as it extends their scope of application.

At minimum, Contracting States shall include as predicate offenses all "serious crime" as well as the express offenses of participation in an organized criminal group, corruption, and obstruction of justice.[100] A "serious crime" is defined as "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty."[101] Contracting States to the Palermo Convention have taken considerably different approaches toward the scope of predicate offenses.[102] As discussed later, the UK and Switzerland are no exception to that.

The scope of reporting obligations is further extended by the obligation that "predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question."[103] However, offenses committed *outside* a Contracting State's jurisdiction qualify as predicate offenses *only if* they are crimes under both the law of the State where committed and the law of the Contracting State applying this article.[104]

As described in more detail later, the qualification of criminal offenses in domestic law as predicate offenses is an important criterion defining the scope of the reporting obligation under the AML/CFT legal framework, which is, therefore, vital in assessing if financial institutions need to report (suspected) violations of export controls and sanctions.

D. Suspicious Activity Reports

SARs are the backbone of FININT.[105] Alongside the reporting obligation, Article 18(b) of the Terrorist Financing Convention obligates Contracting States to adopt domestic legislation requiring their financial institutions "to pay special attention to unusual or suspicious transactions,"[106] meaning to establish internal surveillance systems that identify and flag transactions for potential SARs. This highlights why SARs qualify as "intelligence" rather than just "information," as there exists a process of analysis or evaluation before reporting.[107] However, idiosyncratic for FININT is that this process is carried out by a private-sector actor before the intelligence even reaches a government agency.

Arguably, one reason for outsourcing this intelligence process to financial institutions is to protect financial secrecy,[108] which is prevalent in the financial

100. *Id.* arts. 5, 6(2)(b), 8, 23.
101. *Id.* art. 2(b).
102. Grant & Brent, *supra* note 93, at 6.
103. United Nations Convention Against Transnational Organized Crime, *supra* note 96, art. 6(2)(c).
104. *Id.*
105. Gowhor, *supra* note 91, at 849.
106. International Convention for the Suppression of the Financing of Terrorism, *supra* note 90, art. 18(b).
107. PETER GILL & MARK PHYTHIAN, INTELLIGENCE IN AN INSECURE WORLD 43–44 (2nd ed., 2012).
108. Chat Le Nguyen, *Preventing the Use of Financial Institutions for Money Laundering and the Implications for Financial Privacy*, 21 J. MONEY LAUNDERING CONTROL 47, 47 (2018).

industry in the UK (including its overseas jurisdictions) and Switzerland.[109] A recent example from Germany, yet another jurisdiction with a high financial secrecy,[110] demonstrates that governments expect financial institutions to carry out this duty responsibly. In March 2025, the German financial regulator, for the first time, issued a fine to a supervised firm for repeatedly filing unsubstantiated SARs to the German FIU.[111] This reflects the regulatory expectation that financial institutions must not treat SAR filing as a mere formality, but are required to conduct sound analysis or evaluation before submitting reports.

Finally, Article 18(b) of the Terrorist Financing Convention also requires Contracting States to adapt their domestic legislation to identify "their usual or occasional customers, as well as customers in whose interest accounts are opened."[112] Like the other measures contained in Article 18(b), this is yet another codified requirement of a measure called "Know Your Customer" ("KYC") recommended by the FATF. KYC information is part of FININT,[113] as it may be included in SARs or provided to authorities upon request.[114]

However, it is important to note that FININT goes beyond SARs and KYC. Zarate adopted a broad definition of FININT:

> [A]ny bit of information—however acquired—that reveals commercial or financial transactions and money flows, asset and capital data, and the financial and commercial relationships and interests of individuals, networks, and organizations. Such information can come in a variety of forms: crumpled receipts found in terrorist safe houses, the detailed ledgers of hawaladars, suspicious transaction reports from banks, and transnational wire-transfer records.[115]

The United States, for instance, tapped the intra-bank messaging system operated by the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") to access transnational wire-transfer records as a source of FININT.[116] In contrast to SARs, though, obtaining such records through subpoenas (in this case, under U.S. law) represents a pull, rather than a push mechanism.[117] Nonetheless, it represents another vital path for governments to obtain FININT.

---

109. *Financial Secrecy Index*, TAX JUST. NETWORK (last updated June 3, 2025), https://perma.cc/YHP8-59XZ; *UK Network Remains Biggest Financial Secrecy Supplier Despite Reining In*, TAX JUST. NETWORK (May 22, 2022), https://perma.cc/8UHL-ZSX6.

110. *Financial Secrecy Index*, *supra* note 109.

111. *Ratepay GmbH: BaFin setzt Bußgeld fest*, BAFIN (Mar. 6, 2025), https://perma.cc/8KQV-2WJK.

112. International Convention for the Suppression of the Financing of Terrorism, *supra* note 90, art. 18(b).

113. Gowhor, *supra* note 91, at 849.

114. Ben Scott & Mark McGodrick, *Financial Intelligence and Financial Investigation: Opportunities and Challenges*, 13 J. POLICING INTEL. & COUNTER TERRORISM 301, 301 (2018).

115. ZARATE, *supra* note 85, at 46.

116. Amicelle, *supra* note 76, at 88. SWIFT maintains data operation centers in the Netherlands, Switzerland, and the United States, where data is stored. *Frequently Asked Questions*, SWIFT, https://perma.cc/J7YV-AE5Z.

117. Amicelle, *supra* note 76, at 88.

E. Reporting Obligations for Export Controls and Sanctions in Public International Law

Although the Terrorist Financing Convention was adopted to curb the financing of terrorism, one does not have to look far to make a connection to export controls. The Convention obligates its Contracting States to criminalize offenses stipulated in other treaties listed in its annex,[118] *inter alia* the Convention on the Physical Protection of Nuclear Material ("CPPNM").

The CPPNM obliges Contracting States to refrain from exporting, importing, or authorizing the export or import of nuclear material intended for peaceful purposes unless they have received assurances that the material will be protected during international transport in accordance with the protection levels set out in the CPPNM's annexes.[119]

The CPPNM outlines several serious offences involving nuclear material. These include the unlawful receipt, possession, use, transfer, alteration, disposal, or dispersal of such material when it causes or is likely to cause death, serious injury, or significant property damage.[120] It also criminalizes the theft, robbery, embezzlement, or fraudulent acquisition of nuclear material, as well as acts involving coercion or intimidation to obtain it.[121] Additionally, making threats to use nuclear material to harm people or property, or to commit theft in order to pressure individuals, organizations, or states into certain actions or inactions, also constitutes a punishable offence.[122]

Both the UK and Switzerland are Contracting States to the CPPNM.[123] Therefore, if transposed into domestic legislation as required, financial institutions in both countries have the obligation to assess if funds stem from these criminal offenses and report their suspicions to their respective FIUs under their AML/CFT legal frameworks if the reporting threshold is met.

The Terrorist Financing Convention and the treaties mentioned in its annex are examples of a growing body of transnational criminal law, which "consists of (a) horizontal international obligations between states to criminalize and cooperate, and (b) the vertical application of criminal law and procedures by those states to individuals in order to meet these international obligations."[124]

Since the Convention indirectly imposes obligations on financial institutions through transposition into domestic law, it also takes a place in international financial law. However, within that area of law, the Convention stands out, as most

118. International Convention for the Suppression of the Financing of Terrorism, *supra* note 90, art. 2(1)(a).

119. *See generally* Ronald J. Bettauer, *The Convention on the Physical Protection of Nuclear Material*, 74 AM. J. INT'L L. 205 (1980).

120. Convention on the Physical Protection of Nuclear Material art. 7(1)(a), Mar. 3, 1980, 1456 U.N.T.S. 124.

121. *Id.* arts. 7(1)(b)–(d).

122. *Id.* art. 7(1)(e).

123. *Convention on the Physical Protection of Nuclear Material*, U.N. TREATY COLLECTION, https://perma.cc/7R5G-UQTX.

124. NEIL BOISTER, AN INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW 18 (2nd ed., 2018).

agreements affecting financial institutions promulgate global rules and standards as "informal, non-binding 'soft law' agreements,"[125] which, too, was the case for the FATF Recommendations before UNSCRs 1617 and 2462.

The Terrorist Financing Convention is important for the enforcement of export controls and sanctions, as it has, on the one hand, established a legal framework for states to obtain FININT based on the criminal offenses they deem necessary for their financial institutions to report as SARs. As discussed later, this may also include violations of export controls and sanctions. On the other hand, there exist, to date, no express reporting obligations for financial institutions under binding public international law on export controls and sanctions.

State obligations in binding public international law to implement export controls for certain goods and technology in domestic legislation can notably be found in UNSCR 1540,[126] the Chemical Weapons Convention ("CWC"),[127] and the Arms Trade Treaty ("ATT").[128] The UK and Switzerland are both Contracting States to the CWC[129] and the ATT.[130] However, these obligations grant states discretion if and to what extent they want to directly obligate their financial institutions to report suspected violations of export controls, as there are no such obligations under these agreements.

Among international sanctions, UNSCR 1874 on DPRK distinguishes itself, as it expressly addresses UN member states' "nationals and entities under their laws (including branches abroad), or persons or financial institutions in their territory" and prohibits, *inter alia*, the provision of financial services that "could contribute to the DPRK's nuclear-related, ballistic missile-related, or other [WMD]-related programs or activities."[131] It is accompanied with the obligation for states to apply "enhanced monitoring to prevent all such transactions in accordance with their national authorities and legislation."[132] However, in line with UNSCR 1540, the CWC, and the ATT, UNSCR 1874 also does not contain any reporting obligations for financial institutions. Subsequent UNCRs contain further prohibitions on financing and financial services[133] but also lack reporting obligations.

Although, as discussed earlier, UNSCR 2462 obligates all UN member states to implement the FATF Recommendations, including the recommendations on PF,[134]

125. CHRIS BRUMMER, SOFT LAW AND THE GLOBAL FINANCIAL SYSTEM 3 (2nd ed., 2015).

126. S.C. Res. 1540, ¶ 3, U.N. Doc. S/RES/1540 (Apr. 28, 2004). In 2022, the mandate of UNSCR 1540 was extended for ten years until 2032. *See* S.C. Res. 2663, U.N. Doc. S/RES/2663 (Nov. 30, 2022).

127. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction art. VI(2), Jan. 13, 1993, 1974 U.N.T.S. 45.

128. Arms Trade Treaty art. 5(2), Apr. 2, 2013, 3013 U.N.T.S. 269.

129. *3. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction*, U.N. TREATY COLLECTION, https://perma.cc/H7AP-2AUM.

130. *8. Arms Trade Treaty*, U.N. TREATY COLLECTION, https://perma.cc/ZK2T-QZYU.

131. S.C. Res. 1874, ¶ 18, U.N. Doc. S/RES/1874 (June 12, 2009).

132. *Id*. "Enhanced monitoring" is not defined in the resolution.

133. Wang, Zhu & Zhang, *supra* note 2, at 278.

134. Initially, only FATF Recommendation 7 referred to PF. However, in October 2020, the FATF adjusted Recommendations 1 and 2 to require states and their financial institutions to "identify, assess,

these recommendations refer to the implementation of UNSCR 1718 from 2006 on the DPRK and its current and future successor resolutions, including UNSCR 1874.[135] As mentioned before, these resolutions, on their own, do not contain any reporting obligations.[136]

However, the FATF recommends states to require their financial institutions to "report to competent authorities any assets frozen or *actions taken in compliance with the prohibition requirements of the relevant Security Council resolutions, including attempted transactions*, and ensure that such information is effectively utilised by competent authorities."[137]

But as this reporting obligation currently only applies to financial sanctions against the DPRK,[138] its scope is very narrow, and, as discussed later in the context of reporting obligations for financial sanctions against Russia, it may come in the form of an express reporting obligation in domestic sanctions legislation, while the sanctions violation itself may also qualify as a predicate offense for ML.

Since there is no international convention on PF,[139] FININT on PF in the broader context relies on instruments of transnational criminal law like UNSCR 1540, the Terrorist Financing Convention, and treaties referred to in its annex like the CPPNM, as well as the CWC, ATT, Biological Weapons Convention ("BWC"),[140] and Nuclear Non-Proliferation Treaty ("NNT"),[141] which obligate their Contracting States to criminalize certain conduct relating to the proliferation of WMD.[142] These are imperative to ensure that FININT on these matters can be obtained through the AML/CFT legal frameworks if states do not exercise their discretion to implement express reporting obligations under their export control and sanctions legislation, as the PF-related prohibitions are transposed into criminal offenses under domestic

---

and understand their [PF] risks i.e., the risk of potential breaches, non-implementation or evasion of the targeted financial sanctions" in Recommendation 7 and "take effective mitigation measures." FIN. ACTION TASK FORCE, *supra* note 38, at 6.

135. FIN. ACTION TASK FORCE, *supra* note 89, at 56. Simultaneously, the FATF recommends states to "adopt appropriate measures for monitoring, and ensuring compliance by, financial institutions . . . with the relevant laws or enforceable means governing the obligations under Recommendation 7. *Id*. Failure to comply with such laws, or enforceable means should be subject to civil, administrative or criminal sanctions." *Id*. Reporting and consequences for failure to report are not expressly mentioned.

136. In the context of intelligence, though, it is worth highlighting that the FATF recommends states to have "having appropriate legal authority, and procedures or mechanisms, *to collect or solicit as much information as possible from all relevant sources* to identify persons and entities that, based on reasonable grounds, or a reasonable basis to suspect or believe, meet the criteria for designation in the relevant Security Council resolutions." *Id*. at 55 (emphasis added).

137. *Id*. at 56 (emphasis added).

138. *Id*. at 53 n.19.

139. Wang, Zhu & Zhang, *supra* note 2, at 277.

140. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163.

141. Treaty on the Non-Proliferation of Nuclear Weapons, July 1, 1968, 21 U.S.T. 483, 729 U.N.T.S. 161.

142. *See* de Koker, *supra* note 2, at 127–29. *See also* FIN. ACTION TASK FORCE, *supra* note 89, at 53 n.22 (expressly mentioning that the UNSCR 1540, CWC, BWC, and NNT *do not* fall within the scope of FATF Recommendation 7).

export control and sanctions legislation and result in potential predicate offenses for ML.[143]

Therefore, to understand the role of financial institutions in enforcing export controls and sanctions, it is critical to (1) understand their reporting obligations under *domestic* export control and sanctions legislation (Part II), and (2) to what extent the reporting obligation under the AML/CFT legal framework, as required under public international law, complements the reporting of (suspected) violations of export controls and sanctions (Part III).

III. REPORTING OBLIGATIONS UNDER EXPORT CONTROL AND SANCTIONS LEGISLATION

A. Reporting Obligations Under Export Control Legislation

The UK export control regime relies on one single act: the Export Control Act ("ECA") 2002.[144] ECA 2002 limits the power of the government to those set out in the Act, EU legislation, or international obligations of the UK.[145] It distinguishes between export controls, transfer controls, technical assistance controls, and trade controls.[146]

Export controls refer to goods specified as "military equipment," "goods on which military technology is recorded or from which it can be derived," or "goods intended, designed or adapted for use in the development or production of military equipment or military technology."[147] Trade controls are intended for the acquisition, disposal, or movement of such goods, or the facilitation of such activities,[148] even when these goods do not enter or leave the UK.

Transfer controls refer to technology, which is defined as either "military technology" or "technology intended, designed or adapted for use in the development or production of military technology."[149] Finally, technical assistance refers to "services which are provided or used, or which are capable of being used, in connection with the development, production or use of any goods or technology."[150] The goods and technology refer to those defined under export controls and transfer controls, respectively.

ECA 2002 empowers the government to enact controls should their absence have "relevant consequences."[151] The Secretary of State determines whether an activity involving goods, technology, or technical assistance of any particular description is capable of having a "relevant consequence."[152]

143. *See* note 65.
144. Export Control Act 2002, c. 28 (UK). As opposed to the Swiss export control regime, which relies on two separate acts. Fazzi, *supra* note 35, at 104.
145. Export Control Act 2002, §§ 5(1)–(2).
146. *Id.* §§ 1–4.
147. *Id.* § 1(2), sch. 1, para. 1(1).
148. *Id.* § 4(2), sch. 1, para. 1(1).
149. *Id.* § 2(2), sch. 1, para. 1(2).
150. *Id.* § 3(2), sch. 1, para. 1(3).
151. *Id.* sch. 1, para. 2.
152. *Id.* sch. 1, para. 3(3).

These consequences include an adverse effect on the national security of the UK or its dependencies or on the security of armed forces of the UK or any friendly state; an adverse effect on peace, security, or stability in any region or country; the facilitation, development, production, or use of WMDs; acts threatening international peace and security, violating the law of armed conflict, involving internal repression, or breaching human rights; and the commission or facilitation of terrorism or serious crime anywhere in the world.[153]

ECA 2002 is the basis for the Export Control Order ("ECO") 2008[154] and the Export of Radioactive Sources (Control) Order ("ERSCO") 2006.[155] While the former establishes controls for military and dual-use items, sets out licensing requirements, and creates provisions on offenses, enforcement, and penalties for violations, the latter founds controls for radioactive sources. Both Orders designate His Majesty's Revenue and Customs ("HMRC") for criminal enforcement.[156]

Export controls for dual-use goods are also found in the Council Regulation (EC) No 428/2009 ("Dual-Use Regulation"), which the UK retained post-Brexit.[157] Similarly, the retained Regulation (EU) No 258/2012 of the European Parliament and of the Council ("Firearms Regulation") governs the export of firearms for civilian use.[158] Notably, both Regulations have not been amended yet post-Brexit and are only applicable to Great Britain.[159]

Like in Switzerland,[160] export control legislation in the UK does not contain reporting obligations for financial institutions, although the ECA 2002 expressly allows for the establishment of such. Section 7(1) of ECA 2002 empowers the Secretary of State with the creation of orders with provisions[161]

- requiring persons to provide information to any person specified in the order;[162]

153. *Id.* paras. 3(1)–(2).

154. Export Control Order 2008, S.I. 2008/3231 (UK).

155. Export of Radioactive Sources (Control) Order 2006, S.I. 2006/1846 (UK).

156. Export Control Order 2008, *supra* note 154, art. 41(1); Export of Radioactive Sources (Control) Order 2006, *supra* note 155, art. 12(3). HMRC is a "competent authority" under the Agreement on Police Cooperation between the UK and Switzerland. Agreement on Police Cooperation, *supra* note 32, art. 3(1)(a)(ii).

157. Council Regulation 428/2009, Retained EU Regulation 428/2009 as amended, Dual-Use Regulation (Gr. Brit.).

158. Regulation 258/2012, Retained EU Regulation 258/2012, Firearms Regulation (Gr. Brit.) [hereinafter Firearms Regulation].

159. A third retained EU regulation based on ECA 2002 and only applicable to Great Britain is the Anti-Torture Regulation, which will not be discussed in this article. However, it is part of export control legislation, as it introduced export controls on goods that could be used for the purpose of torture or other cruel, inhuman or degrading treatment or punishment, including capital punishment. *See* Regulation 2019/215, Retained EU Regulation 2019/215, S.I. 2020/1479 (Gr. Brit.).

160. Fazzi, *supra* note 35, at 104.

161. Export Control Act 2002, *supra* note 144, § 1(1).

162. *Id.* § 7(1)(d).

- about the purposes for which information held in connection with anything done under or by virtue of the order may be used;[163] and
- about the persons to whom any such information may be disclosed.[164]

Based on these provisions, ECO 2008 gives the government the power to inspect export-related records.[165] Specifically, if a person is legally required to keep records, under the Order itself or under the Dual-Use Regulation, they must allow an "authorised official" (appointed by the Secretary of State or HMRC) to inspect and copy those records on site.[166] ERSCO 2006 provides for the same power for the Secretary of State or HMRC.[167]

Similarly, the Firearms Regulation allows the Secretary of State (but not HMRC), to ensure that the Regulation is properly applied, to take the necessary and proportionate measures to

- gather information on any order or transaction involving firearms, their parts and essential components and ammunition;[168] and
- establish that the export control measures are being properly applied, which may, in particular, include the power to enter the premises of persons with an interest in an export transaction.[169]

Regulation 15(1) of the Firearms Regulation is worded broadly and could, in theory, be used to justify obtaining information from financial institutions to enforce the Regulation, subject to necessity and proportionality. However, the Dual-Use Regulation contained a similar provision in Regulation 21, which was removed with the Trade etc. in Dual-Use Items and Firearms etc. (Amendment) (EU Exit) Regulations 2019 when Brexit was implemented.[170]

The comparable provisions established in Article 31 of ECO 2008 replaced Regulation 21 of the Dual-Use Regulation, as the amendment was made in the course of the implementation of Brexit. From that, it stands to reason that Regulation 15(1) of the Firearms Regulation is intended to allow the government to inspect export-related records from license holders. However, it is unclear for what reason Regulation 21 of the Dual-Use Regulation has been transposed into ECO 2008, while Regulation 15 of the Firearm Regulation has not.

---

163. *Id.* § 7(1)(e).
164. *Id.* § 7(1)(f).
165. Export Control Order 2008, *supra* note 154, art. 31.
166. *Id.*
167. Export of Radioactive Sources (Control) Order 2006, *supra* note 154, arts. 7(3)–(4).
168. Firearms Regulation, *supra* note 158, reg. 15(1)(a).
169. *Id.* reg. 15(1)(b).
170. Trade etc. in Dual-Use Items and Firearms etc. (Amendment) (EU Exit) Regulations 2019, S.I. 2019/771 (Gr. Brit.).

The Explanatory Note in the Trade etc. in Dual-Use Items and Firearms etc. (Amendment) (EU Exit) Regulations 2019,[171] which amended both the Dual-Use and Firearm Regulations, and the Export Control (Amendment) (EU Exit) Regulations 2022, which amended ECO 2008, are silent on the matter.[172] Similarly, the debates in the UK Parliament on these Regulations do not provide any insights.[173]

B. The Creation of the Office of Trade Sanctions Implementation

In a February 2025 letter from the Chief Executive and First Permanent Secretary of HMRC to the Chair of the Treasury Select Committee of the House of Commons, HMRC clarified its role in the enforcement of export controls and trade sanctions.[174] HMRC stated:

> As part of its statutory functions as the UK customs authority, HMRC is responsible for enforcing both fiscal and non-fiscal trade controls at the UK border (in partnership with Border Force), including trade sanctions and strategic export controls (which have strong similarities both in terms of the legal framework and enforcement methods) . . . In respect of trade sanctions, HMRC is responsible for enforcing sanctions on the import and export of goods and the provision of associated services (e.g. brokering and financial services), as well as the transfer of technology from the UK.[175]

HMRC's letter was a response to an inquiry from the Treasury Select Committee on the role of the Office of Trade Sanctions Implementation ("OTSI") vis-à-vis HMRC. The creation of OTSI was announced on December 11, 2023, with the aim "to crack down on companies dodging Russian sanctions."[176] OTSI is part of the Department for Business and Trade and operates under the authority of the Secretary of State.[177] Its mission was described as follows:

> OTSI will be responsible for the civil enforcement of trade sanctions, including those against Russia. The unit will help businesses comply with sanctions

171. *Id.* Explanatory Note.

172. Export Control (Amendment) (EU Exit) Regulations 2022, S.I. 2022/1300, Explanatory Note (UK).

173. HL Deb (2 Dec. 2020) (808) cols. 194GC–204GC; HC Deb (8 Dec. 2020) cols. 1–12.

174. *See generally* Letter from Sir Jim Harra, Chief Executive and First Permanent Secretary, HM Revenue & Customs, to Dame Meg Hillier, Chair of the Treasury Select Committee, House of Commons (Feb. 17, 2025) (available at https://perma.cc/AF4Q-9YMP) [hereinafter Letter from Sir Jim Harra].

175. *Id.* at 2.

176. Press Release, Dep't for Business & Trade, Off. of Trade Sanctions Implementation, Foreign, Commonwealth & Dev. Off. & Nusrat Ghani MP, New Unit to Crack Down on Firms Dodging Russian Sanctions (Dec. 11, 2023), https://perma.cc/6PVZ-6EHS [hereinafter Crack Down on Russian Sanctions Press Release].

177. Unlike HMRC, the Department for Business and Trade, and thereby by extension OTSI, is not a "competent authority" under the Agreement on Police Cooperation between the UK and Switzerland. Agreement on Police Cooperation, *supra* note 32, art. 3(1)(a).

> and investigate potential breaches, issuing civil penalties and referring cases to HMRC for criminal enforcement where needed. Its remit will involve activity by companies who may be avoiding sanctions by sending products through other countries.[178]

Just six days prior to the announcement, the National Economic Crime Centre, a multi-agency unit in the NCA, HM Treasury's Office of Financial Sanctions Implementation ("OFSI") and the Foreign, Commonwealth & Development Office, had issued a Red Alert on the export of high-risk goods.[179] The purpose of the Alert was to "provide information to UK businesses on common techniques suspected to be in use to evade sanctions on the export of high-risk goods, which Russia is using on the battlefield in Ukraine" with the Alert primarily addressing the UK's financial sector.[180]

To address the important question on OFSI's obvious overlap with HMRC's role in enforcing trade sanctions (but notably not export controls), HMRC clarified in its February 2025 letter:

> OTSI is responsible for civil enforcement of other types of trade sanctions (e.g. sanctions on standalone services, technical assistance and the movement of goods which do not cross the UK border) and can refer serious cases to HMRC for consideration of criminal enforcement action . . . HMRC welcomes the establishment of OTSI to lead on the civil enforcement of trade sanctions that fall outside HMRC's customs remit (i.e. do not involve goods crossing the UK border) and perform other valuable functions in relation to licencing, guidance, raising awareness and business outreach.[181]

The creation of OTSI required a legal basis before it could become operational.[182] This basis was established with the Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations ("TASSCER") 2024, which entered into force on October 10, 2024.[183] TASSCER 2024 created reporting obligations for "certain businesses to provide information, if they suspect a breach has occurred," which applies to financial service providers, money service businesses, and legal service providers.[184]

The legal basis for TASSCER 2024 is not ECA 2002 but the Sanctions and Anti-Money Laundering Act ("SAMLA") 2018.[185] TASSCER 2024 empowers

---

178. Crack Down on Russian Sanctions Press Release, *supra* note 176.

179. *See generally* NAT'L CRIME AGENCY, NAT'L ECON. CRIME CTR., JOINT MONEY LAUNDERING INTEL. TASK FORCE, OFF. OF FIN. SANCTIONS IMPLEMENTATION, HM TREASURY, RED ALERT: EXPORTING HIGH RISK GOODS (2023), https://perma.cc/N4EJ-VJAU.

180. *Id.* at 2.

181. Letter from Sir Jim Harra, *supra* note 174, at 2.

182. Crack Down on Russian Sanctions Press Release, *supra* note 176.

183. Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, S.I. 2024/948 (UK).

184. *Introducing OTSI*, OFF. OF TRADE SANCTIONS IMPLEMENTATION BLOG (Oct. 11, 2024), https://perma.cc/HQZ2-R37E.

185. Sanctions and Anti-Money Laundering Act 2018, c. 13 (UK).

OTSI, as mentioned in the Regulation's title, with the enforcement of the trade, aircraft, and shipping sanctions.[186] These types of sanctions are all defined in SAMLA 2018.[187]

As under ECO 2008, the Secretary of State (but not HMRC) has the power to request information from a person, if it believes that the person may be able to provide the information.[188] This information may be requested for the purpose of the exercise of functions under TASSCER 2024, monitoring compliance with, or detecting evasion of, sanctions regulations, or investigating a suspected breach of a prohibition, or a suspected failure to comply with an obligation, imposed by or under sanctions regulations.[189]

In contrast to the export control legislation, TASSCER 2024 contains reporting obligations both for trade sanctions[190] and aircraft and shipping sanctions.[191] Both of these obligations apply to different persons. However, only the obligation for trade sanctions applies to banks.[192] Regulation 15(1) of TASSCER 2024 stipulates that a

> relevant person ("RP") must inform the Secretary of State as soon as practicable if—
>
> (a) RP knows, or has reasonable cause to suspect, that a person ("P") has breached a prohibition or failed to comply with an obligation under trade sanctions regulations, and
>
> (b) the information or other matter on which the knowledge or cause for suspicion is based came to RP in the course of carrying on their business.[193]

A "relevant person" is defined in Regulation 15(4) and, *inter alia*, includes a person that has permission under Part 4A of the Financial Services and Markets Act ("FSMA") 2000[194] to carry on one or more regulated activities (permission to carry on a regulated activity).[195] This includes banks, as per their definition under

---

186. Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, *supra* note 183, regs. 6–7.

187. Sanctions and Anti-Money Laundering Act 2018, *supra* note 185, §§ 5–7.

188. Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, *supra* note 183, reg. 17(1).

189. *Id.* reg. 17(2).

190. *Id.* reg. 15.

191. *Id.* reg. 16.

192. Since "financial institutions" under UK law encompasses a variety of different legal persons in the financial sector, often with different legal and regulatory obligations, the article will, hereinafter, for greater certainty use the narrower definition of "banks."

193. *Id.* reg. 15(1).

194. Financial Services and Markets Act 2000, c. 8 (UK).

195. Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, *supra* note 183, reg. 15(4), ¶ 4.

the Banking Act 2009, albeit limited to the regulated activity of accepting deposits.[196] Simultaneously, the definition excludes building societies, credit unions, and insurers that accept deposits.[197]

Further, TASSCER 2024 clarifies that the reporting requirement applies to UK persons outside of the UK.[198] In their report to the Secretary of State when complying with their reporting obligation, UK banks must state the information or other matter on which the knowledge or suspicion is based, and any information it holds about a person ("P") by which this person can be identified.[199] Failing to comply with the reporting obligation constitutes an offense.[200]

With the introduction of TASSCER 2024, UK banks are under a broad obligation to report suspected violations of trade sanctions, regardless of their regime. The Regulations also introduced broad powers to disclose sanctions-related information obtained by the Secretary of State to other persons[201] or to the Secretary of State from other persons,[202] which facilitates the exchange of information between HMRC and OTSI.

While HMRC explained in its letter that both HMRC and OTSI have each a distinct role to play in the enforcement of trade sanctions, the letter did not explain whether there exist overlaps in reporting suspected violations of these sanctions to both government agencies. To answer this question, the analysis will turn to reporting obligations under SAMLA 2018.

C. Reporting Obligations under Sanctions Legislation

In contrast to its Swiss counterpart,[203] SAMLA 2018 gives the UK government great discretion to impose sanctions for various purposes such as to comply with UN or other international obligations, or to prevent terrorism, protect national security, promote international peace and security, advance UK foreign policy, resolve armed conflicts, protect civilians, ensure accountability for or deter gross human rights violations, promote compliance with international human rights or humanitarian law, prevent the spread of WMD, and support democracy, the rule of law, and good governance.[204] While "UN obligation" refers to a UNSCR,

196. Banking Act 2009, c. 1, § 2(1) (UK).

197. *Id.* § 2(2); Banking Act 2009 (Exclusion of Insurers) Order 2010, S.I. 2010/35, art. 2 (UK). Analogous to this definition, the BFSA specifies that any financial services supplier in the UK that aims to provide its banking services (i.e., deposit-accepting and lending) cross-border in Switzerland under the Agreement must be incorporated in or formed under the domestic law of the UK and authorized to provide deposit-taking services to the public on a commercial basis in the UK. Berne Financial Services Agreement, Annex 2, arts. III(A), IV(B). Notably, the authorization requirement does not apply to lending services.

198. Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, *supra* note 183, regs. 3(1), 3(3)(a).

199. *Id.* reg. 15(2).

200. *Id.* reg. 15(3).

201. *Id.* reg. 27.

202. *Id.* reg. 28.

203. Fazzi, *supra* note 35, at 105–06.

204. Sanctions and Anti-Money Laundering Act 2018, c. 13, §§ 1(1)–(2).

"international obligation" refers to an obligation of the UK created or arising by or under any international agreement.[205]

Section 5 of SAMLA 2018 defines that sanctions are "trade sanctions" if they impose prohibitions or requirements for one or more of the purposes mentioned in Part 1 of Schedule 1.[206] These purposes are very broad and generally aim to restrict the export, import, movement, transfer, availability, and acquisition of certain goods, services, technologies, land, and cultural property connected to designated persons or prescribed countries.[207] They also cover restrictions on military-related activities, sectoral engagement, infrastructure projects, and compliance with UN measures, particularly those involving ships and cultural objects.[208] In addition, SAMLA 2018 allows Regulations to reference ECO 2008 and the Dual-Use Regulation.[209] These provisions ensure that the references automatically include amendments made in these export control regulations.

HMRC's overlap in enforcing trade sanctions with OTSI stems from the legal framework of trade sanctions under SAMLA 2018. Like the Embargo Act in Switzerland,[210] SAMLA 2018 constitutes the legal basis for country-specific sanctions. However, unlike in its Swiss counterpart, the responsibility for the enforcement of these sanctions is not defined in SAMLA 2018 itself, but rather in the regulations that encompass the country-specific sanctions. Section 17(2) of SAMLA 2018 specifies that regulations based on it may make provision for the enforcement of any prohibitions or requirements imposed by regulations or for preventing such prohibitions or requirements from being circumvented.[211]

Analogous to ECA 2002, regulations under SAMLA 2018 may make provision for requiring or authorizing persons of a prescribed description to inform an appropriate authority of prescribed matters or to create and retain registers or records, authorizing an appropriate authority to require such persons to provide information or produce documents of a prescribed description, conferring powers to inspect and copy prescribed documents or information, conferring powers of entry in relation to such powers, and authorizing or restricting the disclosure of information including provisions about the purposes for which the information may be used and the persons to whom it may be disclosed.[212] The powers conferred to OTSI in TASSCER 2024 notably rely on Section 16(1) of SAMLA 2018.

The Russia (Sanctions) (EU Exit) Regulations 2019 ("Russia Sanctions Regulations"), arguably the UK's most extensive country-specific sanction regime at the moment, exemplify the designation of the criminal enforcement and reporting obligations (or the absence thereof) in regulations under SAMLA 2018.

205. *Id.* § 1(8).
206. *Id.* § 5(1).
207. *Id.* sch. 1, pt. 1.
208. *Id.*
209. *Id.* sch. 1, paras. 21–22.
210. Fazzi, *supra* note 35, at 103.
211. Sanctions and Anti-Money Laundering Act 2018, *supra* note 185, §§ 17(2)(a), (c).
212. *Id.* § 16(1).

As in ECO 2008 and ERSCO 2006, HMRC is tasked with criminal enforcement of the Regulations, albeit mostly and most importantly limited to the trade sanctions under Part 5 thereof.[213]

The trade sanctions under Part 5 of the Russia Sanctions Regulations constitute the largest type of sanctions in the Regulations. At the time of the writing, these trade sanctions contain twenty-five different categories of goods and technology, *inter alia*, luxury goods, iron and steel products, gold, metals, or revenue-generating goods.[214] Some categories make direct reference to ECO 2008 and the Dual-Use Regulations.[215] Most of the twenty-five categories prohibit the provision of financial services relating to these goods and technology.[216]

"Financial services" are defined in Section 61(1) of SAMLA 2018 and consist of a non-exhaustive list of insurance- and banking-related services.[217] The latter includes basic banking services such as accepting deposits, lending, and payment and money transmission services.[218] This differs from the provision of "financial assistance" under EU sanctions against Russia, which *does not* cover payment processing.[219] Additionally, although less relevant to banks, the Russia Sanctions Regulations prohibit the provision of certain services such as interception and monitoring services, internet services, or professional and business services.[220]

However, unlike the financial sanctions under Part 3 of the Regulations,[221] they do not contain any reporting obligations for trade sanctions. Trade license holders are obligated to keep a register or record,[222] which may be inspected and copied by an "authorised official" (appointed by the Secretary of State or HMRC) on site.[223]

Further, Regulation 75 of the Russia Sanctions Regulations empowers HMRC to utilize information powers in the Customs and Excise Management Act 1979 to investigate activities under the Regulations that require a trade license.[224] Any person involved in such activities must provide HMRC with information relating to the goods or the transaction, in such form and within such time as HMRC may reasonably require.[225] Additionally, if requested by HMRC, that person must produce or arrange for the production of any related documents for inspection, either at their principal place of business or another reasonably specified location, and at a time reasonably determined by HMRC.[226]

213. The Russia (Sanctions) (EU Exit) Regulations 2019, SI 2019/855, regs. 85(1), (3)(a) (UK).
214. *Id.* pt. 5.
215. *Id.* reg. 21.
216. *Id.* pt. 5.
217. Sanctions and Anti-Money Laundering Act 2018, *supra* note 185, § 61(1).
218. *Id.* §§ 61(1)(i)–(ii), (iv).
219. Rosneft Oil Co. v. Her Majesty's Treasury, Case C-72/15, EU:C:2017:183 ¶ 184 (Grand Chamber Mar. 8, 2017).
220. The Russia (Sanctions) (EU Exit) Regulations 2019, *supra* note 213, regs. 46K, 54A, 54C, 54D.
221. *Id.* regs. 70, 70ZA, 70A.
222. *Id.* reg. 76.
223. *Id.* reg. 77.
224. *Id.* reg. 75.
225. Customs and Excise Management Act 1979, c. 2, § 77A(1)(a) (UK).
226. *Id.* § 77A(1)(b).

Therefore, the absence of reporting obligations for trade sanctions in the Russia Sanctions Regulations underscores the need for the reporting obligations in TASSCER 2024. HMRC's letter highlights that information obtained through OTSI represents a vital source of potential violations of sanctions and even export controls through reference to ECO 2008 and the Dual-Use Regulations in sanctions regulations, where applicable. HMRC stipulated:

> We have worked closely with OTSI to establish an enforcement partnership (including a Memorandum of Understanding) whereby OTSI will refer serious cases to HMRC for consideration of criminal enforcement action, in accordance with our published criminal investigations policy. HMRC will review all referrals we receive from OTSI and adopt cases that we consider to be suitable for criminal investigation.[227]

In addition, HMRC listed out the methods it uses to detect sanction breaches, which includes "[b]usinesses self-reporting breaches to HMRC through the voluntary disclosure process" and "[r]eceiving actionable intelligence from UK law enforcement authorities, the intelligence community and international counterparts."[228] However, the reliance on *voluntary* disclosure from businesses, rather than *mandatory* direct reporting from businesses, including banks, aligns with the finding that reporting obligations for trade sanctions are absent in the Russia Sanctions Regulations. Simultaneously, the reference to "intelligence from UK law enforcement authorities" adumbrates HMRC's reliance on the NCA's FININT.

Compared to Switzerland, the UK has established a more robust legal framework that explicitly requires banks to report suspected violations of trade sanctions.[229] Prior to the enactment of TASSCER 2024, the legal frameworks in both jurisdictions were remarkably similar. First, neither of them imposed reporting obligations under their respective export control legislation. Second, reporting duties under sanctions regimes, such as those relating to Russia, were limited to financial sanctions, e.g., asset freezes. Third, no mandatory reporting regime for suspected breaches of trade sanctions was in place.

With the introduction of TASSCER 2024, the UK has addressed this legal gap by imposing a general reporting obligation for suspected violations of trade sanctions across all sanction regimes. In contrast, this gap still persists in Switzerland.[230] There, financial institutions may be required to report such suspicions under the AML/CFT framework, but only where specific statutory thresholds for a SAR are met.[231]

Moreover, the legal framework governing the enforcement and reporting of trade sanctions in the UK is structured inversely to that of Switzerland. In

227. Letter from Sir Jim Harra, *supra* note 174, at 2.

228. *Id*. at 3.

229. The Swiss sanctions against Russia only contain a reporting obligation for crude oil and petroleum products, while there exist no reporting obligations for armaments, high-tech goods, or other categories of goods. Fazzi, *supra* note 35, at 105.

230. *Id*. at 110.

231. *Id*. at 106–08.

Switzerland, the authority to initiate criminal proceedings for breaches of trade sanctions is set out in the Embargo Act,[232] the Swiss counterpart to SAMLA 2018. By contrast, in the UK, such enforcement responsibilities are assigned at the level of secondary legislation, such as the Russia Sanctions Regulations.

Similarly, reporting obligations in Switzerland are established through secondary legislation (i.e., ordinances, the Swiss equivalent of regulations in the UK).[233] While the UK framework theoretically allows for reporting obligations to be codified in individual regulations, as demonstrated by the inclusion of reporting obligations in the Russia Sanctions Regulations for financial sanctions, the UK has adopted a more consolidated and pragmatic approach. Under TASSCER 2024, the reporting of suspected breaches of trade sanctions is now mandated uniformly across all UK sanctions regimes. This type of centralized solution would also be legally and administratively feasible in Switzerland through the enactment of a federal ordinance.

Unlike SAMLA 2018, the Swiss Embargo Act does not confine trade sanctions to pre-defined categories. This legislative flexibility has arguably afforded Switzerland greater discretion in transposing the EU's sanctions against Russia into domestic law, sparing the Federal Council the challenge of adapting EU measures to a rigid typology through secondary legislation.

Nevertheless, while SAMLA 2018 prescribes specific types of sanctions, it also confers broad discretion on the UK to tailor sanctions for a wide range of foreign policy and national security objectives. By contrast, Switzerland's legal framework restricts its capacity to impose sanctions to those mandated by the United Nations or the Organisation for Security and Co-operation in Europe ("OSCE"), or to the transposition of measures adopted by its most significant trading partners, such as the EU.[234]

IV. AML/CFT REPORTING OBLIGATIONS

A. Reporting Obligations Under AML/CFT Legislation

The reporting of suspected violations of export controls and sanctions under the AML/CFT legal framework in the UK complements, analogous to Switzerland,[235] the reporting of suspected violations under the export control and sanctions legislation.[236] However, the AML/CFT reporting mechanism plays a much more important role in Switzerland in the absence of reporting obligations

232. *Id.* at 102.
233. *Id.* at 104–06.
234. *Id.* at 103.
235. *Id.* at 106–07.
236. It is important to bear in mind that reporting obligations for AML are different than for CFT, as both frameworks serve different purposes. However, the previous sections highlighted that under public international law, both frameworks are intertwined and the UNSCRs relating to terrorism and the Terrorist Financing Convention have done much to render AML obligations under public international law legally binding to all UN member states. Therefore, it should not come to a surprise that both the UK and Switzerland each have codified AML and CFT obligations into one single primary act, which justifies referring to AML/CFT legislation instead of just AML legislation.

for financial institutions in the export control and sanctions legislation.[237] In the UK, as discussed, banks are already obligated to report suspected violations of trade sanctions under TASSCER 2024.

Nonetheless, the AML/CFT legal framework complements the reporting under TASSCER 2024 in two distinct ways. First, as discussed, export control legislation in the UK does not contain any reporting obligations for banks for suspected violations of export controls. Second, the AML/CFT legal framework extends the scope of the reporting obligation to suspected violations of export controls and sanctions under foreign law, e.g., under U.S. law, EU law, Swiss law, or even law of the People's Republic of China, in alignment with the requirements in the Palermo Convention.

SAMLA 2018 stands out in comparison to the Swiss legal framework, as it substantively combines elements that, in Switzerland, are separated between the Embargo Act and the Anti-Money Laundering Act ("AMLA"). However, in contrast to Part 1 of SAMLA 2018, which governs sanctions, the AML/CFT provisions in Part 2 appear relatively concise. The Swiss AMLA is extensive by comparison.

Section 49(1) of SAMLA 2018 permits an "appropriate Minister" to make provision for "enabling or facilitating the detection or investigation of money laundering, or preventing money laundering" or "the implementation of Standards published by the Financial Action Task Force from time to time relating to combating threats to the integrity of the international financial system."[238] Analogous to the Swiss AMLA, "money laundering" is not defined in SAMLA 2018 itself but in the act that codifies the offense: Section 340(11) of the Proceeds of Crime Act ("POCA") 2002.[239] Section 340(11) refers to Sections 327, 328, and 329 of the Act.[240] POCA 2002 effectively transposed the UK's criminalization of ML obligation under the Palermo Convention into UK domestic law.[241]

Under Section 327, ML comprises concealing, disguising, converting, transferring, or removing criminal property from England and Wales, Scotland, or Northern Ireland.[242] Under Section 328, ML is if a person (i.e., the bank employee) enters into or becomes concerned in an arrangement which they know or suspect facilitating (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person.[243] Under Section 329, the acquisition, use, or possession of criminal property also constitutes ML.[244] All three sections are subject to multiple exceptions.

---

237. *Id.*
238. Sanctions and Anti-Money Laundering Act 2018, *supra* note 185, §§ 49(1)(a), (c).
239. *Id.* § 49(3).
240. Proceeds of Crime Act 2002, c. 29, § 340(11) (UK).
241. Png, *supra* note 54, at 27–28.
242. Proceeds of Crime Act 2002, *supra* note 240, § 327(1).
243. *Id.* § 328(1).
244. *Id.* § 329(1).

Subparagraphs (b) to (d) of Section 340(11) extend the definition of ML for offenses by including not only the direct commission of the offense, but also attempts, conspiracies, or incitement to commit it; acts of aiding, abetting, counselling, or procuring its commission; and conduct that would amount to any of these offenses if committed within the UK, even if done abroad.[245]

"Criminal property" is defined in Section 340(3) of POCA 2002. Property is criminal property if it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and the bank employee knows or suspects that it constitutes or represents such a benefit.[246] "Property" is defined broadly. Besides money, it includes all forms of property, real or personal, heritable or moveable; and things in action and other intangible or incorporeal property.[247] "Property" must be criminal at the time the alleged ML has been committed.[248]

"Benefit," too, is defined broadly in POCA 2002.[249] Its concept is extremely complex and subject to evolving case law.[250] According to Rudi Fortson, "benefit" includes

> not only the property that the offender obtained as a result of or in connection with the offence, but also any "pecuniary advantage" that he or she obtained from it (for example the value of tax or duty evaded, or the value of a debt deferred). It is immaterial who carried out the criminal conduct, or who benefited from it, or whether the criminal conduct occurred before or after POCA 2002 came into force.[251]

The obligation to report ML is contained in Sections 330–332, split into obligations for the regulated sector, nominated officers in the regulated sector, and other nominated officers.[252] The following discussion will focus on the reporting obligation in Section 330, as it applies to every person in a bank.

Unlike the Swiss AMLA,[253] POCA 2002 formulates reporting obligations solely in negative terms. Rather than imposing affirmative duties to report, it establishes criminal liability for failures to report in specified circumstances, thereby framing compliance through the lens of omission-based offenses. The report (i.e., "disclosure") must be made either to a "nominated officer" or to a person authorized by the NCA.[254]

---

245. *Id.* §§ 340(11)(b)–(d).
246. *Id.* § 340(3).
247. *Id.* § 340(9).
248. R v GH, [2015] UKSC 24 [47]–[48].
249. Proceeds of Crime Act 2002, *supra* note 240, §§ 340(5)–(7).
250. Rudi Fortson, *Money Laundering Offences Under POCA 2002*, *in* BANKS AND FINANCIAL CRIME: THE INTERNATIONAL LAW OF TAINTED MONEY 149–52 (2nd ed. William Blair, Richard Brent & Tom Grant eds., 2017).
251. *Id.* at 149.
252. Proceeds of Crime Act 2002, *supra* note 240, §§ 330–332.
253. Fazzi, *supra* note 35, at 106.
254. Proceeds of Crime Act 2002, supra note 240, § 330(4).

Three conditions must be met for the reporting obligation under Section 330 of POCA 2002 to be triggered. First, the bank employee must know, suspect, or have reasonable grounds to know or suspect that another individual is engaged in ML.[255] Second, the relevant knowledge or suspicion must arise from information or material obtained in the course of a business operating within the regulated sector.[256] Third, the employee must either be able to identify the suspected individual or the location of the laundered property, or reasonably believe that the information obtained may assist in such identification.[257] This framework imposes an implicit due diligence obligation on the bank employee, requiring them to assess whether the information encountered in the course of their work gives rise to a duty to file a SAR.

Analogous to Switzerland,[258] courts have assisted in determining the threshold for the reporting of suspicion. However, unsurprisingly, the case law in the UK on this matter is far more developed. With its ruling in *R v. Da Silva*, the Court of Appeal set the bar for reporting low. Suspicions exist if there is a "possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice."[259] In *K Ltd v. National Westminster Bank Plc & Ors*, the Court of Appeal further stipulated:

> The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect he must (either himself or through the bank's nominated officer) inform the authorities.[260]

Both judgments were positively cited by the Court of Appeal in *Shah v. HSBC*.[261] However, as commented by Paul Marshall, "the decision in *Shah* has raised the prospect, for the first time, of the maker of a SAR being put to proof of the grounds of their suspicion," since the Court of Appeal had determined that an individual who is the subject of a SAR is entitled to have the grounds for the suspicion disclosed.[262]

Marshall highlighted that when the AML regime was introduced in 2003, the prudent advice of lawyers has been to file a SAR in case of doubt.[263] However, the decision in *Shah* put banks in a dilemma of either risking criminal liability for not reporting as soon as practicable or civil liability for breach of contract,[264]

255. *Id.* § 330(2).
256. *Id.* § 330(3).
257. *Id.* § 330(3A).
258. Fazzi, *supra* note 35, at 107–08.
259. R v. Da Silva, [2006] EWCA (Crim) 1654 [16].
260. K Ltd. v. Nat'l Westminster Bank plc, [2006] EWCA (Civ) 1039 [21].
261. Shah & Anor v. HSBC Private Bank (UK) Ltd, [2012] EWHC (QB) 1283 [67]–[68].
262. Paul Marshall, *Does Shah v HSBC Private Bank Ltd Make the Anti-money Laundering Consent Regime Unworkable?*, 25 BUTTERWORTHS J. INT'L BANKING & FIN. L. 287, 288–89 (2010).
263. *Id.* at 289.
264. *Id.*

since POCA 2002, unlike the Swiss AMLA, did not contain an exclusion of liability provision when satisfying the obligation to file a SAR. This effectively hindered the gathering of FININT.[265]

To remedy this shortcoming, Marshall suggested "to introduce an express statutory protection for those in the regulated sector against civil claims where a SAR is made in good faith,"[266] as recommended by the FATF.[267] This recommendation was realized with the Serious Crime Act 2015 and the introduction of Section 338(4A).[268] Although it remains difficult for banks in practice to determine where the thin line between "more than fanciful" and "vague feeling of unease" lies,[269] documenting the grounds for suspicion following *Shah* serves to demonstrate that the bank has acted in good faith when filing a SAR.

In contrast to the Swiss AMLA, POCA 2002 contains two express exceptions for the obligation to report. A person is exempt from the obligation if they have a "reasonable excuse" for not making the required disclosure or if they have not been provided training by their employer.[270] In absence of jurisprudence and regulatory guidance on what constitutes a "reasonable excuse," views differ from extreme circumstances such as duress or threats to safety to when the information to be reported to the FCA lies in the public domain.[271]

Analogous to Switzerland,[272] POCA 2002 permits filing SARs in case of suspected ML even if the requirements under the obligation to report are not satisfied. In the UK, this "right to report" is found in Section 337 named "protected disclosures."[273] These disclosures are a protection from committing an offense under Section 330.[274]

The requirements for the "right to report" directly align with the requirements for the failure to disclose in Section 330, with exception of the missing third condition in Section 330, i.e., that the bank employee must either be able to identify

265. *Id.*

266. *Id.*

267. FIN. ACTION TASK FORCE, *supra* note 89, at 19.

268. Proceeds of Crime Act 2002, *supra* note 240, § 338(4A). However, section 338 relates to "authorised disclosures," while the obligation to report discussed so far are "required disclosures." Both of them qualify as SARs, but with different purposes. Required disclosures "are triggered where a reporter knows or suspects, or has reasonable grounds to know or suspect (whether or not they do, in fact, suspect) that a person is engaged in money laundering." L. COMM'N, ANTI-MONEY LAUNDERING: THE SARS REGIME 40–41, ¶ 2.4(1) (2019), https://perma.cc/EZ4G-93YZ. They "provide law enforcement agencies with intelligence opportunities to disrupt criminality." *Id.* In contrast, "authorised disclosures . . . are most commonly triggered if, in a professional capacity, a reporter encounters suspected criminal property. *Id.* at 41, ¶ 2.4(2). These SARs have a dual function. First, they provide the investigative authorities with details of a reporter's suspicion of criminal property." *Id.* Second, they allow the NCA to "grant the reporter consent to carry out an otherwise prohibited act by, for example, allowing the suspicious transaction to take place." *Id.* There is no such distinction in the Swiss AMLA.

269. Marshall, *supra* note 262, at 289.

270. Proceeds of Crime Act 2002, *supra* note 240, §§ 330(6)(a), (c), (7).

271. L. COMM'N, *supra* note 268, at 56, ¶ 3.20.

272. Fazzi, *supra* note 35, at 109.

273. Proceeds of Crime Act 2002, *supra* note 240, § 337.

274. *Id.* Explanatory Note, ¶ 491.

the suspected individual or the location of the laundered property, or reasonably believe that the information obtained may assist in such identification. This requirement is absent in the "right to report" in Section 337. As in the Swiss AMLA,[275] the express protection from civil liability enshrined in Section 338(4A) for the obligation to report is absent in the "right to report."[276]

Sections 327–329 of POCA 2002 contain limitations as to what constitutes a predicate offense, i.e., if the relevant criminal conduct is "not of a description prescribed by an order made by the Secretary of State."[277] These limitations transposed the requirement under the Palermo Convention that "predicate offences shall include offences committed both within and *outside the jurisdiction of the State Party in question*."[278] However, this only applies if the offense committed abroad constitutes an offense in the UK as well.[279]

In contrast to Switzerland,[280] the UK also obligates banks to file a SAR even if the offense is lawful in the jurisdiction where the offense has been committed but is unlawful in the UK if the "conduct which would constitute an offence punishable by imprisonment for a maximum term in excess of 12 months in any part of the United Kingdom."[281] With this, the UK has effectively exceeded its obligations under the Palermo Convention and rendered the reporting obligation under the AML/CFT legislation for banks broader than in Switzerland.

Only offenses in three Acts were expressly excluded: offenses under the Gaming Act 1968,[282] under the Lotteries and Amusements Act 1976,[283] and under Sections 23 and 25 of the FSMA 2000.[284] The latter comprises carrying out a regulated financial activity and performing a controlled function within a regulated firm without approval from the FCA, respectively.[285]

In *El-Khouri v. Government of the United States*, a 2025 case, the UK Supreme Court clarified the limits of extraterritorial applicability of the POCA 2002. While predicate offenses may be committed outside the UK, the act of ML itself must occur within the UK.[286] Thereby, the Supreme Court overturned an earlier decision of the Court of Appeal in which a UK citizen residing in Spain was convicted of ML for paying funds into a Spanish bank account he obtained from defrauding persons in the UK.[287]

---

275. Fazzi, *supra* note 35, at 109.
276. *See* note 268.
277. Proceeds of Crime Act 2002, *supra* note 240, §§ 327(2A)(b)(ii), 328(3)(b)(ii), 329(2A)(b)(ii).
278. United Nations Convention Against Transnational Organized Crime, *supra* note 96, art. 6(2)(c) (emphasis added).
279. *Id.*
280. Fazzi, *supra* note 35, at 108.
281. The Proceeds of Crime Act 2002 (Money Laundering: Exceptions to Overseas Conduct Defence) Order 2006, S.I. 2006/1070, art. 2(2) (UK).
282. Gaming Act 1968, c. 65 (Gr. Brit.), repealed by Gambling Act 2005, c. 19 (Gr. Brit.).
283. Lotteries and Amusements Act 1976, c. 57 (Gr. Brit.), repealed by Gambling Act 2005, c. 19 (Gr. Brit.).
284. Financial Services and Markets Act 2000, *supra* note 194, §§ 23, 25.
285. *Id.*
286. El-Khouri v. Government of the United States, [2025] UKSC 3 [75].
287. *Id.* at [80].

B. Predicate Offenses in Export Control and Sanctions Legislation

The connection between ML and sanctions becomes evident with the UK's first-ever conviction of Russian sanction breaches in April 2025.[288] A Russian offender with UK citizenship managed to open an account at a UK bank whilst under financial sanctions by the UK.[289] After his non-sanctioned wife paid GBP 75,000 into his account, the bank realized that their client was sanctioned, froze the assets, and reported the client.[290]

The offender was "found guilty of eight counts of intentionally participating in activities that knowingly would breach Russian sanctions and two counts of money laundering related offences and has been sentenced to 40 months imprisonment."[291] His ML convictions underscore that the sanction breach constituted a predicate offense.

Just five months prior in December 2024, the public disclosure of the NCA's "Operation Destabilise" also demonstrated the obvious links between ML, sanctions evasion, organized crime, and hostile state activity (i.e., illicit Russian activities) on UK soil, and, thus, their relevance to UK intelligence.[292]

In the operation, the NCA targeted groups that provided ML services to sanctioned oligarchs, Russian elites, ransomware operators, and organized crime networks.[293] The laundered funds were used to support Russian espionage operations across Europe and to amplify Russian disinformation and misinformation campaigns.[294] Five natural and four legal persons have been sanctioned subsequently by the United States, including a Thai-based legal entity accused of having exported electrical components to Russia.[295] The Royal United Services Institute ("RUSI") summarized the case by emphasizing that "the UK system must be fit for purpose to combat threats that blur the lines between criminal and foreign intelligence operations."[296]

From a legal perspective, the AML/CFT framework *is* already fit for purpose, as predicate offenses in the UK also encompass export controls and trade sanctions, not just financial sanctions. Offenses relating to export, transfer, technical assistance, and trade controls are contained in Article 34 of ECO 2008. The Regulation contains two offenses that may result in imprisonment for a term not exceeding two years: a WMD-related offense and a military end-use offense.[297]

288. Press Release, Crown Prosecution Serv., Sentencing: The First Ever UK Prosecution of Russian Sanction Breaches (Apr. 11, 2025), https://perma.cc/B5RV-TZQ7 [hereinafter Crown Prosecution Press Release]. Between 2021 and 2024, HMRC only referred three cases to prosecution. Letter from Sir Jim Harra, *supra* note 174, at 7.

289. Crown Prosecution Press Release, *supra* note 288.

290. *Id.*

291. *Id.*

292. Jamie MacColl & Kathryn Westmore, *Operation Destabilise: Russia, Organised Crime and Illicit Finance*, ROYAL UNITED SERVS. INST. (Dec. 6, 2024), https://perma.cc/TC9P-YBWG.

293. *Id.*

294. *Id.*

295. *Id.*

296. *Id.*

297. Export Control Order 2008, *supra* note 154, art. 34(4)(b).

A person commits an offense if they breach an export, transfer, or technical assistance control knowing, being aware, or having grounds to suspect that the goods, software, or technology are or may be intended for WMD purposes, even in part.[298] Similarly, a person commits an offense if they breach an export or transfer control after being informed by the Secretary of State that the dual-use goods, software, or technology pursuant to these controls are or may be intended for use by a military end-user listed in Regulation 12A, which supplements the Dual-Use Regulation.[299]

Furthermore, a third offense covers all types of controls under ECO 2008. A person knowingly concerned in an activity prohibited by export, transfer, technical assistance, or trade controls with the intent to evade the relevant prohibition commits an offense.[300] The contravention of a prohibition or restriction in the Dual-Use Regulation on WMD purposes, end-use control or brokering services, or failure to comply with the requirement to notify the Secretary of State in case of awareness of end-use for certain military or WMD purposes in the Dual-Use Regulation also constitutes an offense.[301]

Under the Dual-Use Regulation, a person knowingly concerned in an activity prohibited or restricted by Regulations 3(1), 4(1), 4(2), 4(3), and 5(1) commits an offense.[302] The former four Regulations relate to the requirement of an export authorization for (1) listed dual-use items, (2) non-listed dual-use items if the exporter has been informed by the Secretary of State they may be intended for WMD-related purposes, (3) non-listed dual-use items if intended for military end-use if the destination is subject to an arms embargo, and (4) non-listed dual-use items if the exporter has been informed by the Secretary of State that the items, wholly or partly, are for use as parts or components of military items in Schedule 2 of ECO 2008 previously exported without authorization.[303] Regulation 5(1) imposes the same prohibition for exporters in Article 4(1) for non-listed dual-use items intended for WMD-related purposes onto brokers.[304]

Finally, both ECO 2008 and ERSCO 2006 contain offenses relating to misleading applications for licenses and failure to comply with license conditions.[305] By comparison, offenses pertaining to violations of trade sanctions under the Russia Sanctions Regulations are easily described. Any offense against the trade sanctions (Part 5 of the Regulations) is contained in one provision: Regulation 80(2).[306]

298. *Id*. art. 34(3).
299. *Id*. art. 34(3A).
300. *Id*. art. 34(5).
301. *Id*. art. 35(2).
302. *Id*. art. 35(4).
303. Dual-Use Regulation, *supra* note 157, regs. 3(1), 4(1)–(3).
304. *Id*. reg. 5(1).
305. Export Control Order 2008, *supra* note 154, arts. 37(1), 38(1); Export of Radioactive Sources (Control) Order 2006, *supra* note 155, arts. 9(1), 10(1).
306. The Russia (Sanctions) (EU Exit) Regulations 2019, *supra* note 213, reg. 80(2).

12. Practical Issues with Enforcement

Releasing their findings at an opportune moment, Allison and Keatinge from RUSI reported on the role of financial institutions in enforcing trade sanctions against Russia in the UK in March 2025.[307] Their findings are based on anonymized interviews with more than twenty compliance personnel in banks, financial technology companies, and sanctions compliance service providers.[308] In their policy brief, they note:

> [Financial Institutions' ("FIs'")] compliance systems have been built at great cost over a long period of time, mostly to respond to regulations against money laundering, terrorist financing and corruption. These systems cannot be quickly changed or adapted to respond to regulators' new focus on trade.[309]

However, this statement overlooks an important fact. It is correct that banks' compliance systems have been built over a long period of time because they were responses to comply with their obligations under AML/CFT legislation. As discussed in this article, all UN member states, including the UK and Switzerland, have had the obligation to impose such legislation since 9/11 in 2001.

However, Contracting States to the Palermo Convention have also had the obligation to introduce a wide range of predicate offenses for ML. For the UK and Switzerland, this obligation has existed since 2006. Such predicate offenses may include violations of trade sanctions or export controls, which, as demonstrated, is the case for the UK and Switzerland. Therefore, banks' obligation to assess whether funds relating to the trade of goods or services stem from criminal activity and report their suspicions to a FIU is nothing new and has not emerged recently in response to the sanctions against Russia.

Similarly, Hilgenstock *et al.* recommend that "financial institutions should be tasked to play a key role in the monitoring of trade in export-controlled goods and in impeding illicit transactions,"[310] failing to highlight that banks *are* already legally tasked with the enforcement of export controls and sanctions, albeit contingent on their host state's implementation of its AML/CFT obligations under public international law.[311]

---

307. Allison & Keatinge, *supra* note 2.
308. *Id.*
309. *Id.*
310. Hilgenstock et al., *supra* note 2, at 194.
311. This connection is also absent in Stewart, Viski & Brewer's article on PF. *See* Stewart, Viski & Brewer, *supra* note 2, at 1109 (concluding that "national legislation [on PF] is often lacking and inadequate, and where it exists, is often poorly implemented, and in practice, controls on [PF] are inadequate," a situation that "contrasts with implementation of controls on [ML] and terrorist financing, which have become central to state financial regulatory requirements, and corresponding private sector financial compliance efforts, in recent years," but without addressing that PF-related conduct may indirectly give rise to reporting obligations under the AML/CFT framework). *But see* Wang, Zhu & Zhang, *supra* note 2, at 278 (noting that in "China, because specific laws and regulations on [PF] are lacking, [AML/CFT] provisions are usually used when dealing with the issue").

Rather, RUSI's findings adumbrate that banks have not sufficiently paid attention to their role in the enforcement of export controls and sanctions, as it noted:

> While FIs' compliance personnel understand this and express commitment to complying with G7 sanctions, there is a limit to how much disruption they (and their boards) are willing to impose on their corporate clients, many of whom have a higher risk tolerance than the FIs.[312]

"Disruption," here is meant to be understood, although rather cryptically, as the willingness to take the mandatory due diligence measures to identify and mitigate the risks from ML and PF,[313] which inevitably requires the information and cooperation of bank customers. As opposed to Swiss banks,[314] UK banks already have the express obligation to identify and mitigate risks pertaining to PF, notably since September 1, 2022,[315] which previously implicitly have been contained in ML risks.[316]

It is difficult to assess whether the unwillingness to "disrupt" customers effectively stems from banks' compliance officers, their senior management, their boards, or a combination thereof. However, as per a survey by PwC in 2024, only 36% of banks in the UK believe that the current AML rules are useful.[317] PwC attributes UK banks' attitude to the fact that they have traditionally been the primary focus of the FCA and are subject to substantial penalties for non-compliance with AML/CFT regulations.[318]

A central issue for banks is to decide if funds stemming from transactions relating to the trade of goods or services infringe export control or sanctions legislation. Among RUSI's interviewees' complaints was the lack of engagement and detailed guidance regarding the expectations of sanctions authorities from the United States, UK, and EU, which would facilitate banks' decision-making.[319]

Under UK law, banks must ensure that their employees are "made aware of the law" relating to ML and PF and are "regularly given training in how to recognise and deal with transactions and other activities or situations" which may be related to these risks.[320] However, it stands to reason that this obligation to educate

312. Allison & Keatinge, *supra* note 2.

313. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, SI 2017/692, regs. 18–19 (UK).

314. Fazzi, *supra* note 35, at 106–07.

315. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, *supra* note 313, regs. 18(A), 19(A).

316. Furthermore, banks have the obligation to ensure that their subsidiaries and branches outside the UK in countries with weaker requirements than the UK apply measures equivalent to those in the UK. *Id.* reg. 20(3).

317. PWC, PWC EMEA AML SURVEY 2024: UK INSIGHTS ON EFFECTIVENESS 9 (2024), https://perma.cc/7F8Z-UBG9.

318. *Id.*

319. *See also* de Koker, *supra* note 2, at 137–38; Weise, Hund & Carr, *supra* note 2, at 130–31.

320. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, *supra* note 313, reg. 24(1)(a).

employees poses a challenge to banks in the UK, analogous to banks in Switzerland.[321]

Indeed, export controls and sanctions *are* complex areas of law,[322] and RUSI's reference to U.S. and EU sanctions implicitly refers to UK banks' obligation to also detect and report violations of *foreign* sanction legislation to counter ML. Nonetheless, it must be highlighted once more that the evasion and circumvention of export controls and sanctions are not new concepts or issues.[323]

Banks cannot rely on the complexity of export controls and sanctions as a justification for failing to provide training in these areas of law. While the ever-changing and evolving nature of these areas of law introduces a significant degree of legal uncertainty, this does not absolve banks of their obligation to educate staff adequately and oblige them to report funds stemming from suspected violations of export controls or sanctions,[324] particularly when provisions have been made to protect them from civil liability when such reports under the AML/CFT framework are made in good faith. Moreover, the banks' customers operating in the manufacturing or trade of goods that are subject to export control or sanctions obligations are not exempt from this legal expertise either.[325]

Rather, banks' disinterest in prioritizing the enforcement of export controls and sanctions is arguably part of a broader problem with their AML/CFT obligations. As described in another RUSI publication from 2019, financial regulators have traditionally emphasized strict rule compliance, penalizing banks for any missteps, which has pushed banks to over-report to avoid penalties.[326] Consequently, banks prioritize avoiding penalties and safeguarding their reputation over genuinely reducing ML.[327] Unsurprisingly, the inefficiencies of the AML/CFT reporting obligations in the UK have been the subject of numerous

321. *See* de Koker, *supra* note 2, at 142 (noting that "few compliance officers would have the technical expertise to identify that a trade transaction involves goods that may not be listed but may still be used for proliferation purposes"); Fazzi, *supra* note 35, at 108–09; Wang, Zhu & Zhang, *supra* note 2, at 282 (noting that in China, "financial institutions do not have the necessary expertise to use the export control system").

322. de Koker, *supra* note 2, at 141; Fazzi, *supra* note 35, at 108–09; Zolandz & Noorbaloochi, *supra* note 2, at 395–96.

323. Andy Caines, *Sanctions and Export Control Evasion Techniques and Practical Steps to Identify, Assess and Mitigate Risk*, 8 J. FIN. COMPLIANCE 317, 319 (2025).

324. *See* Zolandz & Noorbaloochi, *supra* note 2, at 398 (noting that "[c]ompliance professionals with a deep understanding of sanctions regulations and the methods employed for circumvention are essential for effectively interpreting the data generated by screening systems and making informed decisions about potential sanctions risks. Training should be provided to all appropriate employees on a periodic basis and tailored to the organisation's risk profile").

325. *See* de Koker, *supra* note 2, at 141–42. *See also id.* at 147 (highlighting that mining and engineering companies as well as universities would typically have a low customer risk profile for AML/CFT, but their PF risk profile may be "much higher").

326. MATTHEW REDHEAD, ROYAL UNITED SERVS. INST., DEEP IMPACT? REFOCUSING THE ANTI-MONEY LAUNDERING MODEL ON EVIDENCE AND OUTCOMES viii (Oct. 19, 2019), https://perma.cc/P9ZZ-3QW3.

327. *Id.*

scholarly articles,[328] and this article does not intend to contribute to this ongoing discussion.

Nonetheless, two facts deserve to be highlighted. First, between 2020 and 2022, the number of SARs submitted to the NCA increased from 573,085 to 901,255,[329] reflecting a trend of growing SARs analogous to Switzerland.[330] Second, the number of cases and arrests resulting from SARs is remarkably low. In 2018, the NCA received 463,938 SARs, which resulted in only 40 arrests in 28 ML cases.[331] However, the NCA did not report the number of arrests and cases in 2022.[332] While these numbers provide insights into the NCA's inefficiency of turning SARs into prosecutions of ML, criminal proceedings are not the only value of SARs. SARs as FININT may also influence policymaking or take on a preemptive role by eliminating threats to the UK and its people.[333]

C. Insights from the Law Commission's Review of the SARs Regime

The deliberation in defining a broad reporting obligation for banks under the AML/CFT legislation was delineated in the Law Commission's 2019 review of the SARs regime.[334] On the growing number of SARs, the Commission noted:

> While there is an understandable desire among those working in law enforcement *to maximise the amount of intelligence and raw data they receive*, a large volume of SARs does not guarantee quality of intelligence.[335]

Simultaneously, the Commission stated that it had "clear confirmation from law enforcement agencies that SARs are a vital source of intelligence" and that "they are one of the primary methods of sharing information to produce intelligence for law enforcement agencies to investigate and prosecute crime more generally."[336]

Like its Swiss counterpart,[337] the NCA faces a growing number of SARs, many of which are of low quality. The Commission identified four main reasons for poor-quality SARs: a low threshold for criminal liability, individual (not

328. *See, e.g.*, Mario Menz, *It Is Best to Say Nothing at All – Suspicious Activity Reporting in the Financial Services Sector*, 31 J. FIN. CRIME 302 (2024); Peter Alan Sproat, *Is the UK's Anti-money Laundering Regime "Worth the Candle"? A Tentative Cost-benefit Analysis*, 26 J. MONEY LAUNDERING CONTROL 1100 (2023); Rafael Pontes, Nick Lewis, Paul McFarlane & Patrick Craig, *Anti-money Laundering in the United Kingdom: New Directions for a More Effective Regime*, 25 J. MONEY LAUNDERING CONTROL 401 (2022); XiaoTong Loh, *Suspicious Activity Reports (SARs) Regime: Reforming Institutional Culture*, 24 J. MONEY LAUNDERING CONTROL 514 (2021).

329. Sproat, *supra* note 328, at 1105.

330. Fazzi, *supra* note 35, at 109. Thus, the trend of decreasing SARs in Switzerland observed prior to 2019, as mentioned by Dabor, no longer applies. *See* Dabor, *supra* note 4, at 8.

331. Jonathan Fisher, *Is the Swamped SARS Regime Efficacious?*, COUNSEL (Apr. 10, 2023), https://perma.cc/XTT6-QURM.

332. *Id.*

333. Ward, *supra* note 1, at 29, ¶ 1.85.

334. L. COMM'N, *supra* note 268.

335. *Id.* at 31, ¶ 1.57 (emphasis added).

336. *Id.* ¶ 1.59.

337. Fazzi, *supra* note 35, at 109.

corporate) liability leading to defensive reporting, confusion over reporting obligations, and misunderstandings about the legal concept of suspicion.[338] This finding highlights that two of the underlying issues stem directly from a lack of understanding of the law, analogous to the lack of understanding of export controls and sanctions legislation.

Therefore, it stands to reason that the way forward is to improve banks' legal expertise and illustrate the value of SARs to banks, aligning with a statement made by Tristram Hicks (former Detective Superintendent on the national Criminal Finance Board), Ian Davidson (former Detective Superintendent with national financial investigation responsibility) and Professor Mike Levi, Cardiff University, on behalf of the Law Commission:

> In our view it would be a better use of time and money to invest in explaining better the known value of SARs through research and routine case reviews than to cut them off at source. This would provide empirical evidence of the utility of SARs to both the reporting sector and to senior managers in law enforcement, *particularly those without investigative or intelligence backgrounds*.[339]

Ironically, the Law Commission opined on the reporting obligation for *legal professionals* that their better understanding of the law resulted in a "disproportionate burden," since they are better suited to identify predicate offenses in transactions, and declared this an "unintended consequence" of the broad reporting obligation.[340] Thereby, the Commission unintentionally confirmed the obvious: knowledge of the law increases the ability to identify predicate offenses, which allows the NCA to receive better SARs (i.e., fewer false positives).

The Commission considered an alternative "serious offenses" approach for SARs whereby banks would only have to report funds stemming from "serious offenses," based on either a pre-defined list of offenses or maximum penalty.[341] This is the approach effectively followed in Switzerland, where banks only have to report funds suspected of stemming from felonies or a pre-defined list of offenses.[342] However, the Commission ultimately recommended maintaining the current approach.[343]

Aligning with the Commission's recommendation, the "serious offenses" approach was also opposed by most respondents. The Crown Prosecution Service argued that under the current approach, banks are not overburdened because they do not have to identify the predicate offense.[344] In agreement, the law firm Freshfields noted that:

338. L. COMM'N, *supra* note 268, at 33–34, ¶ 1.69.
339. *Id.* at 35, ¶ 1.74 (emphasis added).
340. *Id.* at 71, ¶ 4.9.
341. *Id.* at 73, ¶ 4.12.
342. Fazzi, *supra* note 35, at 106.
343. L. COMM'N, *supra* note 268, at 85, ¶ 4.75.
344. *Id.* at 74, ¶ 4.21.

> A narrower definition would mean that, in addition to identifying certain patterns of transactions as indicative of criminal conduct, compliance officers/systems would have to perform an investigative function to link a transaction to a specific crime before filing a SAR . . . [I]t is intelligence agencies, rather than reporting entities, that are best placed and qualified to investigate what the predicate offence which renders property criminal may be in any given context.[345]

Concurring, UK Finance, the British trade association for the UK banking and financial services sector, added that under the suggested "serious offenses" approach, banks "would be unable to consistently determine the predicate offence or the seriousness of the crime."[346]

Finally, government stakeholders, including law enforcement agencies, also supported the current approach, as it results in a "broader intelligence picture" and provides a "'gateway' to disrupt criminality."[347] Conversely, more than half of the respondents that supported moving away from the current approach were from the legal sector,[348] arguably because they *are*, indeed, better equipped to determine the seriousness of a crime.

On February 12, 2024, the UK government concurred with the Law Commission on retaining the current approach.[349] In response to the Law Commission's recommendation, the UK government had established the SARs Advisory Group in May 2021 to continuously improve the quality and effectiveness of SARs, with input from both public and private sector stakeholders.[350] Alongside this, the SARs Reform Programme launched ongoing feedback and engagement initiatives to enhance the understanding of ML threats and improve SAR quality through regular reviews and outreach.[351]

Although the current approach in the UK reduces the burden on banks to identify the exact predicate offense, and government initiatives have aimed to improve the quality of SARs, banks are still required to have a sound understanding of criminal law in order to form a reasonable suspicion that property is criminal in nature and, thus, subject to reporting. This reduces the risk of over-reporting, straining valuable resources of the NCA to identify false positives. This is evident from the NCA's 2023 "Guidance on submitting better quality Suspicious Activity Reports (SARs)," which highlights, through several examples, that a SAR without the reason for the suspicion is of low value.[352]

345. *Id.* ¶ 4.22.
346. *Id.* ¶ 4.23.
347. *Id.* at 75, ¶ 4.27.
348. *Id.* ¶ 4.24.
349. *Response to Law Commission Review of the SARs Regime*, U.K. HOME OFF. (Feb. 12, 2024), https://perma.cc/NLK7-PQLY (archived at UK Nat'l Archives).
350. *Id.*
351. *Id.*
352. U.K. FIN. INTEL. UNIT, NAT'L CRIME AGENCY, GUIDANCE ON SUBMITTING BETTER QUALITY SUSPICIOUS ACTIVITY REPORTS (SARS) 3, 26–28 (2023), https://perma.cc/5A3V-Z86E.

V. PRACTICALENFORCEMENT CHALLENGES AND CONCLUSION

A. Addressing the Practical Issues with Enforcement

Subsequently, banks' assessment of whether funds stem from violations of export controls or sanctions must involve requesting and evaluating supporting documentation such as export documents, bills of lading, certificates of origin, licenses from relevant competent authorities, particularly the provision of harmonized system ("HS") codes of goods, and information on the countries of destination and origin.[353] This allows banks to determine whether the goods or services linked to a transaction are subject to export controls or sanctions and, if so, whether the required licenses have been obtained to ensure the transaction complies with applicable laws.

The Court of Appeal in *R v. Da Silva* expressly mentioned that a case might arise where a bank employee might "entertain a suspicion . . . but, on further thought, honestly dismissed it from his or her mind as being unworthy or as contrary to such evidence as existed or as being outweighed by other considerations."[354] This relates to banks' proactive obligation to request information from their customers to be able to dismiss such suspicions.

Banks must scrutinize transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the bank's knowledge of the customer and the customer's business and risk profile.[355] This applies if the customer carries out an occasional transaction that amounts to a transfer of funds exceeding EUR 1,000 or the bank suspects ML.[356] They are obligated, for instance, to "assess, and where appropriate obtain information on, the purpose and intended nature of the business relationship or occasional transaction."[357] These customer due diligence measures, too, are nothing new, and are rooted in obligations for financial institutions under the Terrorist Financing Convention, which all UN member states must enforce.

Despite the existence of these customer due diligence obligations, RUSI's report stipulates that banks' current compliance systems, according to the survey's respondents, are not tailored towards the enforcement of trade sanctions, which further reinforces the point that banks have not prioritized adopting the enforcement of export controls and sanctions in their daily business. RUSI noted:

> In particular, FIs struggle to implement sanctions that are activity or sector-based, rather than simply lists of names of individuals and entities. For example, trade sanctions target specific categories of goods, most often referring to their six-digit [HS] codes, or to technical specifications of the controlled goods themselves. Financial messaging and payment data rarely includes HS codes

353. Caines, *supra* note 323, at 327–28.
354. R v. Da Silva, [2006] EWCA (Crim) 1654 [17].
355. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, *supra* note 313, , reg. 28(11)(a).
356. *Id.* regs. 27(1)(b)–(c).
357. *Id.* reg. 28(2)(c).

> or detailed goods descriptions, making it difficult to integrate into existing sanctions compliance systems.[358]

However, as argued above, banks' risk of facilitating ML by conducting transactions linked to the trade of goods or services that may violate export controls or sanctions has existed for two decades.[359] The fact that banks have not tailored their compliance systems accordingly points to a failure on the part of these institutions. As aptly summarized by Andy Caines:

> FIs need to approach the recent increase in sanctions circumvention not as a new risk, but rather as a risk that can be mitigated by enhancing existing controls, possibly with new controls being deployed because of the expanding scope and nature of export controls against Russia.[360]

In detail, Caines demonstrates in his publication how banks can adapt their existing controls to mitigate the risk of ML related to export controls and sanctions and, thereby, effectively remedies the alleged absence of government guidance on the topic,[361] as criticized by respondents in RUSI's survey.[362]

Finally, RUSI's respondents' claim that "financial sanctions remain a higher focus (and better understood) than trade sanctions for national authorities" is irrefutable,[363] since the UK had evidently omitted to introduce reporting obligations for trade sanctions for banks when its sanctions against Russia were imposed, as opposed to the reporting obligations for financial sanctions.[364] This was effectively remedied with the establishment of TASSCER 2024 and OTSI, however, notably two and a half years after the introduction of the Russia sanctions.

358. Allison & Keatinge, *supra* note 2.

359. Caines, *supra* note 323, at 324.

360. *Id*. This view is contrasted by Stewart, Viski & Brewer who noted that "there are aspects of [PF] that cannot be addressed by existing AML/CFT tools." Stewart, Viski & Brewer, *supra* note 2, at 1112–13. This divergence may arise from the distinction between a practice-based viewpoint and an academic perspective.

361. Ironically, RUSI and ACAMS reported in their survey that European banks are "the most likely to consult proliferation finance reports published by non-governmental and academic institutions." DALL & WALKER, *supra* note 73, at 4–5.

362. Weise, Hund & Carr, *supra* note 2, at 131 (noting that there is a "dearth of useful, 'actionable' information about what proliferation finance actually looks like"). However, Caines's publication has contributed to remedying that gap. An earlier 2017 report from King's College London has also contributed to closing that gap in literature. *See* JONATHAN BREWER, PROJECT ALPHA, KING'S COLL. LONDON, STUDY OF TYPOLOGIES OF FINANCING OF WMD PROLIFERATION (2017), https://perma.cc/EV8L-S3X6. The lack of awareness that these academic publications exist might be an issue contributing to banks' lacking knowledge on the subject matter.

363. Allison & Keatinge, *supra* note 2.

364. This also supports Weise, Hund & Carr's statement on the disconnect between export controls and combating PF. Weise, Hund & Carr, *supra* note 2, at 130 ("The disconnection between export control and counterproliferation finance (CPF) may stem in part from the perception that the latter CPF refers only to implementation of targeted financial sanctions and not to countering the financing of various proliferation-related activities not yet subject to any [UNSCRs] or [FATF] recommendations").

Nonetheless, TASSCER 2024 should have been the final wake-up call for banks to update their compliance system to identify and mitigate risks stemming from trade sanctions, since the reporting obligations under TASSCER 2024 are not equivalent and are more straightforward than those under POCA 2002. As mentioned earlier, under TASSCER 2024, a bank employee in the course of carrying out their business must inform the Secretary of State as soon as practicable if they know, or have reasonable cause to suspect, that a person has breached a prohibition or failed to comply with an obligation under trade sanctions regulations.[365]

This reporting obligation arguably has a lower threshold than the reporting obligation under POCA 2002, as it is not limited to funds stemming from criminal activity. Rather, the knowledge or suspicion of a violation itself triggers the obligation. However, in contrast to POCA 2002, the obligation only refers to violations of trade sanctions under UK law.

Effectively, TASSCER 2024 has generated a dual-reporting obligation for banks for funds suspected of stemming from a violation of trade sanctions. In absence of jurisprudence on the matter, it is unclear whether submitting a report to the Secretary of State while omitting to file a SAR would constitute a "reasonable excuse" protecting from criminal liability under POCA 2002.[366] Conversely, such a defense is absent in TASSCER 2024. Therefore, a bank that has filed a SAR due to a suspicion but has omitted to do so under TASSCER 2024 could not rely on statutory protection for this omission. Similarly, TASSCER 2024 does not offer a defense to bank employees who have failed to report suspected trade sanctions, but who have not been provided training by their employer, as under POCA 2002.

In its guidance, OTSI lists "good standards of customer due diligence and other relevant compliance systems proportionate to the size, exposure to sanctions and resources of the business" as a mitigating factor in civil enforcement cases, i.e., in "non-serious cases" that are not referred to HMRC for criminal enforcement.[367] This underscores, once again, that banks will inevitably have to improve their expertise in export control and sanctions legislation and adapt their compliance systems to be able to comply with this reporting obligation in order to avoid liability for non-reporting.

B. Conclusion

Compared to Switzerland, the UK has established a legal framework that obligates banks to report FININT on suspected violations of export controls and sanctions through different channels. Through TASSCER 2024, the UK has created a broad reporting obligation that pertains to trade sanctions contained within all sanction regimes of the UK. This approach is notably different than for financial sanctions, whose reporting obligations have been, so far, contained in the regulations

365. Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024, *supra* note 183, reg. 15(1).

366. Proceeds of Crime Act 2002, *supra* note 240, §§ 330(6)(a), (c), (7).

367. Dep't for Bus. & Trade & Off. for Trade Sanctions Implementation, *How Suspected Breaches of Trade Sanctions Are Assessed by the Office of Trade Sanctions Implementation (OTSI)*, GOV.UK (last updated July 31, 2025), https://perma.cc/4CTJ-F48C.

for the specific sanction regimes. This new approach does not only prevent potential gaps in reporting obligations for current or future trade sanctions, as the case for Switzerland's current sanctions against Russia, but it also offers banks greater legal certainty, as the obligation applies uniformly across all sanction regimes.

As in Switzerland, the reporting obligations under the AML/CFT legislation in the UK complement reporting under sanctions legislation, particularly in absence of specific reporting obligations for banks in export control legislation. However, as under sanctions legislation, the UK's AML/CFT legislation goes beyond the reporting obligations for financial institutions in Switzerland. First, under POCA 2002, banks are required to assess if funds stem from criminal activity but are not required to determine the seriousness of the crime to decide if filing a SAR is required. This approach benefits both banks and the NCA, as it eliminates a time-consuming step that financial institutions in Switzerland, in comparison, must undergo. On the other hand, it allows the NCA to obtain more FININT.

Second, the UK's reporting obligation for predicate offenses committed abroad goes beyond the minimum standard under the Palermo Convention, as the POCA 2002 also requires banks to file a SAR if the predicate offense was committed outside the UK in a jurisdiction where the predicate offense was lawful, but if committed in the UK would constitute an offense. This has significant implications for banks' reporting obligations, as it requires them to assess customers' overseas conduct as if it were subject to UK criminal law, including sanctions and export control legislation, for the purposes of identifying and reporting criminal activity, even if the conduct is lawful in the customers' jurisdiction.

Ironically, due to this obligation, banks are subsequently required to determine the seriousness of the crime, since predicate offenses committed abroad that are lawful in the jurisdiction where they were committed only need to be reported if UK equivalent of the offense is punishable by imprisonment for a maximum term in excess of 12 months.

Conversely, to a certain extent, this alleviates banks' obligation to develop an understanding of the criminal law of the jurisdictions in which their customers operate to determine whether a SAR must be filed, since they can use UK criminal law as a benchmark. In comparison, under the Swiss AMLA, which strictly follows the requirements of the Palermo Convention, financial institutions must always be aware whether funds stem from a predicate offense punishable under the laws of the jurisdictions to which their clients are subject and under Swiss law. If not, there is no obligation to report.

Therefore, alongside TASSCER 2024, it stands to reason that the UK has developed legal frameworks for the reporting of suspected violations of export controls and sanctions that are, from a legal perspective, superior to the Swiss frameworks, as the UK does not rely mostly on the AML/CFT framework for FININT thanks to the establishment of TASSCER 2024. The UK AML/CFT framework also has a broader scope of application than its Swiss counterpart, allowing the UK government to obtain more FININT.