Global Investigations Review

The Guide to Sanctions

Editors
Rachel Barnes, Paul Feldberg, Nicholas Turner, Anna Bradshaw, David Mortlock, Anahita Thoms and Rachel Alpert

Second Edition

The Guide to Sanctions

Reproduced with permission from Law Business Research Ltd
This article was first published in July 2021
For further information please contact Natalie.Clarke@lbresearch.com

Editors

Rachel Barnes

Paul Feldberg

Nicholas Turner

Anna Bradshaw

David Mortlock

Anahita Thoms

Rachel Alpert

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as at June 2021, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to:
natalie.hacker@lbresearch.com.
Enquiries concerning editorial content should be directed to the Publisher:
david.samuels@lbresearch.com

ISBN 978-1-83862-596-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

BAKER & HOSTETLER LLP

BAKER MCKENZIE

BARNES & THORNBURG LLP

BDO USA LLP

CARTER-RUCK SOLICITORS

CRAVATH, SWAINE & MOORE LLP

EVERSHEDS SUTHERLAND

FORENSIC RISK ALLIANCE

GLOBAL LAW OFFICE

JENNER & BLOCK LLP

MCGUIREWOODS LLP

MAYER BROWN

MILLER & CHEVALIER CHARTERED

PETERS & PETERS SOLICITORS LLP

SEWARD & KISSEL

SIMMONS & SIMMONS LLP

STEPTOE & JOHNSON

STEWARTS

THREE RAYMOND BUILDINGS

WHITE & CASE LLP

WILLKIE FARR & GALLAGHER LLP

Publisher's Note

The Guide to Sanctions is published by Global Investigations Review – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing.

We live, it seems, in a new era for sanctions: more and more countries are using them, with greater creativity and (sometimes) selfishness.

And little wonder. They are powerful tools. They reach people who are otherwise beyond our jurisdiction; they can be imposed or changed at a stroke, without legislative scrutiny; and they are cheap! Others do all the heavy lifting once they are in place.

That heavy lifting is where this book comes in. The pullulation of sanctions has resulted in more and more day-to-day issues for business and their advisers.

Hitherto, no book has addressed this complicated picture in a structured way. The *Guide to Sanctions* corrects that by breaking down the main sanctions regimes and some of the practical problems they create in different spheres of activity.

For newcomers, it will provide an accessible introduction to the territory. For experienced practitioners, it will help them stress-test their own approach. And for those charged with running compliance programmes, it will help them do so better. Whoever you are, we are confident you will learn something new.

The guide is part of the GIR technical library, which has developed around the fabulous *Practitioner's Guide to Global Investigations* (now in its fifth edition). *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to think about at every stage, You should have both books in your library, as well as the other volumes in GIR's growing library – particularly our *Guide to Monitorships*.

We supply copies of all our guides to GIR subscribers, gratis, as part of their subscription. Non-subscribers can read an e-version at www.globalinvestigationsreview.com.

I would like to thank the editors of the *Guide to Sanctions* for shaping our vision (in particular Paul Feldberg, who suggested the idea), and the authors and my colleagues for the elan with which it has been brought to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher, GIR
June 2021

Contents

Foreword

I am pleased to welcome you to the Global Investigations Review guide to economic sanctions. In the following pages, you will read in detail about sanctions programmes, best practices for sanctions compliance, enforcement cases, and the unique challenges created in corporate transactions and litigation by sanctions laws. This volume will be a helpful and important resource for anyone striving to maintain compliance and understand the consequences of economic sanctions.

The compliance work conducted by the private sector is critically important to stopping the flow of funds to weapons proliferators such as North Korea and Iran, terrorist organisations like ISIS and Hezbollah, countering Russia's continued aggressive behaviour, targeting human rights violators and corrupt actors, and disrupting drug traffickers such as the Sinaloa Cartel. I strongly believe that we are much more effective in protecting our financial system when government works collaboratively with the private sector.

Accordingly, as Under Secretary of the US Department of the Treasury's Office of Terrorism and Financial Intelligence from 2017 to 2019, one of my top priorities was to provide the private sector with the tools and information necessary to maintain compliance with sanctions and AML laws and to play its role in the fight against illicit finance. The Treasury has provided increasingly detailed guidance on compliance in the form of advisories, hundreds of FAQs, press releases announcing actions that detail typologies, and the Office of Foreign Assets Control (OFAC) framework to guide companies on the design of their sanctions compliance programmes. Advisories range from detailed guidance from OFAC and our interagency partners for the maritime, energy and insurance sectors, to sanctions press releases that provide greater detail on the means that illicit actors use to try to exploit the financial system, to Financial Crimes Enforcement Network (FinCEN) advisories providing typologies relating to a wide range of illicit activity.

Whether it was for the Iran, North Korea or Venezuela programmes, or in connection with human rights abuses and corrupt actors around the globe, the US Treasury has been dedicated to educating the private sector so that they in turn can further protect themselves.

The objective is not only to disrupt illicit activity but also to provide greater confidence in the integrity of the financial system, so we can open up new opportunities and access to financial services across the globe. That guidance is particularly important today with the increased use of sanctions and other economic measures across a broader spectrum of jurisdictions and programmes.

As you read this publication, I encourage you to notice the array of guidance, authorities and other materials provided by the US Treasury and other authorities cited and discussed by the authors. This material, provided first-hand from those charged with writing and enforcing sanctions laws, gives us a critical understanding of these laws and how the private sector should respond to them. By understanding and using that guidance, private companies can help to protect US and global financial systems against nefarious actors, as well as avoid unwanted enforcement actions.

Thank you for your interest in these subjects, your dedication to understanding this important area of the law, and your efforts to protect the financial system from abuse.

Sigal Mandelker
Former Under Secretary of the Treasury for Terrorism and Financial Intelligence
June 2021

Part I

Sanctions and Export Control Regimes Around the World

5

UK Sanctions Enforcement

Rachel Barnes, Saba Naqshbandi, Patrick Hill and Genevieve Woods[1]

Introduction

Sanctions enforcement is now firmly placed within the United Kingdom's broader economic crime regime.[2] The Office of Financial Sanctions Implementation (OFSI) in HM Treasury was established in 2016. It aims to 'develop as a world leader in financial sanctions implementation and enforcement'[3] and has signalled an intention robustly to enforce sanctions compliance and to impose significant financial penalties in appropriate cases. In 2017, the maximum term of imprisonment for financial sanctions breaches was increased from two to seven years.[4] Under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA), it is further increased to 10 years.[5] Following Brexit, it is anticipated that the UK's autonomous sanctions regime will expand both in scope and in the number and severity of enforcement actions.

---

1 Rachel Barnes, Saba Naqshbandi, Patrick Hill and Genevieve Woods are barristers at Three Raymond Buildings, London.

2 HM Treasury and HM Home Office 'Economic Crime Plan, 2019 to 2022', 13 September 2019, para. 1.12, at www.gov.uk/government/publications/economic-crime-plan-2019-to-2022. This chapter focuses primarily on financial sanctions enforcement. The new Director of OFSI's role has been expanded to include economic crime policy at HM Treasury. In his first blog, the new Director stated of his twin roles: 'This brings HMT's sanctions policy and operational implementation roles together . . . and integrates them into the government's broader economic crime agenda. . . I hope to use my expanded role to build stronger links between sanctions and broader economic crime work, exploiting the large overlap in threats, issues and stakeholders.' OFSI, An Introduction from new OFSI director Giles Thomson, 4 February 2021, at https://ofsi.blog.gov.uk/2021/02/04/an-introduction-from-new-ofsi-director-giles-thomson/.

3 OFSI, Annual Review April 2018 to March 2019 (October 2019) p. 1, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/838178/Annual_Review_2018-19_FINAL.pdf.

4 Policing and Crime Act 2017 s 144(3)(a), giving government the power to provide for a maximum term of imprisonment in the case of conviction on indictment of seven years in sanctions regulations made under the European Communities Act 1972. The maximum term of imprisonment provided in regulations made under that Act had been two years – see European Communities Act 1972 Sched. 2 para. 1(1)(d) (unamended).

5 Sanctions and Anti-Money Laundering Act [SAMLA] s 17(5)(a).

Offences established under sanctions legislation

Regulations for each sanctions regime prohibit certain conduct (see Chapter 4), creating offences that arise when the prohibited activity is conducted with the requisite mental element (primary offences). In each sanctions regime there is also a set of secondary offences that can be committed in respect of (1) licences applied for or issued to permit otherwise prohibited conduct, and (2) requirements to report or requests to provide information or documents to OFSI.

Primary offences

Examples of primary offences include when a person deals with the funds of a designated person without a licence, knowing or suspecting, or having reasonable grounds to suspect that the relevant transaction is prohibited.[6] A person may be guilty of a circumvention offence when they intentionally participate in activities, knowing that the object or effect is (directly or indirectly) to circumvent any sanctions prohibition or to enable or facilitate the contravention of any such prohibition.[7]

Secondary offences

- *Licensing offences*: (1) failing to comply with any condition of a licence; and (2) knowingly or recklessly providing false information or documentation for the purpose of obtaining a licence.
- *Reporting offences*: failing to inform HM Treasury as soon as practicable if a relevant firm knows or has reasonable cause to suspect that a person is a designated person or has breached financial sanctions regulations and the information on which the knowledge or suspicion is based came to them in the course of carrying on their business.
- *Information offences*: (1) failing to comply with a request by OFSI for information or the production of documents without a reasonable excuse; (2) knowingly or recklessly providing materially false information or documentation in response to such a request;[8] (3) destroying, mutilating, defacing, concealing or removing any document with intent to evade requirements under a request for information or documents; or (4) otherwise intentionally obstructing HM Treasury in respect of its powers to make such a request.[9]

---

6 Exceptions and defences are set out in the regulations for each regime. See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, reg. 81.

7 For a discussion of the limitations of circumventing offences, see R v. R [2015] EWCA Civ 796.

8 As described below, both the Crown Prosecution Service [CPS] and the Serious Fraud Office [SFO] also have powers to compel the provision of information and documents which may be applicable in investigations of suspected offences under sanctions legislation (see section titled 'Investigative powers' below). Along with those powers, the relevant legislation also establishes secondary offences of failing to comply with disclosure or production notices issued by the CPS or SFO and knowingly or recklessly providing materially false or misleading information or documents in response to such notices – see Serious Organised Crime and Police Act 2005 [SOCPA], s 67; Criminal Justice Act [CJA] 1987 s 2(13), (14).

9 Such conduct would amount to a common law offence of perverting the course of justice in the context of an anticipated criminal investigation or when one is known to have commenced. *Vreones* [1891] 1 QB 360; *Government of the USA v. Dempsey* [2018] 4 WLR 110. For the comparable offence in respect of SFO investigations, see CJA 1987 s 2(16).

- *Confidentiality offences*: a person who is provided with specified confidential information or who obtains it commits an offence by disclosing it without lawful authority if that person knows or has reasonable cause to suspect that the information is to be treated as confidential.[10]

The reporting offences can only be committed by the classes of persons specified in the legislation. These include persons subject to (the slightly narrower) anti-money laundering compliance obligations and supervision, and those carrying on regulated activity under the Financial Services and Markets Act 2000, currency exchange or funds transmission businesses, auditors, accountants and legal professionals.[11]

The offences can only be committed if relevant firms fail to disclose information they are obliged to report.[12] For example, if the suspicion of a sanctions breach arose solely from information obtained other than in the course of business, such as through media reporting, then neither the reporting requirement nor the offence would arise. The reporting requirement does not require the disclosure of information that is subject to legal professional privilege (LPP), or information that would be prohibited under data protection legislation or the Investigatory Powers Act 2016.[13] Regulations also provide for exceptions from liability for conduct that would otherwise constitute an offence for breach of the financial restrictions, confidentiality, information or reporting provisions, where a Crown officer acting as such has determined that the conduct would be in the interests of national security or the prevention or detection of serious crime in the UK or elsewhere.[14]

Liability for secondary parties, inchoate offences, corporates and company officers

The ordinary criminal law principles of accessorial liability, inchoate offences and corporate liability (the identification principle)[15] apply. When an offence is committed with the consent or connivance of, or is attributable to the neglect of, any director, manager, secretary or other similar officer of the corporation or a person acting in such a capacity, that person is guilty of the offence in addition to the corporation and is liable to prosecution.[16]

10 See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, reg. 9.

11 A 'relevant firm' is defined in the interpretation provision of each set of sanctions regulations (see, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019), reg. 2.

12 OFSI's Guidance on Financial Sanctions [Financial Sanctions Guidance] contains a list of examples of the kinds of information that must be reported to OFSI: see pp. 21–22. The precise requirements are set out in each set of financial sanctions regulations.

13 For further discussion of legal professional privilege [LPP], see 'Duties of counsel and privilege' below. See also, e.g., Democratic People's Republic of Korea (EU Exit) Regulations 2019, reg. 109.

14 SAMLA s 15(2)(a), (6); see, e.g. Global Anti-Corruption Sanctions Regulations 2021/488, reg. 20; Global Human Rights Sanctions Regulations 2020/680, reg. 19.

15 Also known as the attribution theory of corporate liability. The primary rules of identification may be subject to a more purposive interpretation in respect of regulatory offences, such as sanctions offences, in which the conduct and *mens rea* of a corporate officer other than the directing will and mind of the company as a whole may be attributed to the company to establish liability: see *Meridian Global Funds Management Asia Ltd v. Securities Commission* [1995] 2 AC 500 (PC); *Bilta (UK) Ltd (In Liquidation) v. Nazir* [2016] AC 1; *Serious Fraud Office v. Barclays plc* [2020] 1 Cr App R 28.

16 See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, reg. 111.

Jurisdiction

Jurisdiction is established on the basis of both territory and nationality (active personality). The sanctions regulations impose prohibitions and requirements and establish related offences in relation to conduct in the United Kingdom or its territorial sea by any person and conduct elsewhere by a 'United Kingdom person',[17] defined as a 'United Kingdom national' (which includes British citizens, British subjects and British protected persons)[18] or body incorporated or constituted under the law of any part of the United Kingdom.[19]

Investigations into sanctions offences

Commencement

Investigations may commence following voluntary self-disclosure by a natural or legal person, a report to OFSI or a UK law enforcement agency by a third party such as a whistle-blower, a person's professional regulator, the filing of a suspicious activity report (SAR) to the National Crime Agency (NCA) under money laundering or counter-terrorism laws, or after a UK law enforcement agency receives information from an overseas counterpart or international organisation that violations have or are suspected to have occurred.

Notification

There is no general requirement to notify a suspect of an investigation. A suspect may not be made aware of a criminal investigation until some overt action is taken, such as:

- arrests of individuals;
- service of production orders or information provision notices;
- execution of search warrants;
- if a third party that holds or controls the assets, such as a bank or a trustee, freezes the assets unilaterally by refusing to execute their directions;
- service of a subsequent court order, such as a restraint order issued in the Crown Court or a bank account freezing order by a magistrates' court; or
- if a person has self-reported or disclosed a suspected sanctions breach to OFSI or some other enforcement authority, the authority's response to that disclosure confirming that an investigation has commenced.

Only when OFSI has formed an intention to impose a civil monetary penalty upon a person is it required to inform the person of its intention to do so and provide the person with the opportunity to make representations.[20]

17 SAMLA s 21.

18 SAMLA s 21(3).

19 SAMLA s 21(2). Jurisdiction may be specifically extended to include bodies incorporated or constituted under the laws of any of the Channel Islands, the Isle of Man, or any of the British overseas territories (SAMLA s 21(4)).

20 This procedure is described below in the section titled 'Civil monetary penalties'.

Enforcement authorities

Although OFSI is the primary organisation responsible for sanctions implementation, other relevant agencies include the NCA, the Crown Prosecution Service (CPS), the Serious Fraud Office (SFO), Her Majesty's Revenue and Customs (HMRC),[21] the Export Control Joint Unit of the Department for International Trade,[22] and also professional regulators and overseas enforcement agencies.[23]

OFSI works closely with the NCA, whose sanctions investigations are conducted by its International Corruption Unit.[24] Typically, the NCA refers cases for prosecution to the CPS.[25] The SFO may investigate and prosecute cases in which sanctions offences intersect with international bribery or serious or complex fraud.[26]

> In 2009, the SFO prosecuted Mabey & Johnson Ltd and three executives for breaches of UN Iraq sanctions that were linked to the payment of bribes in exchange for oil contracts.

Investigative powers

In a sanctions investigation, OFSI may use its powers to require persons to provide information to detect evasion and to investigate offences. Requests will be made in writing and will specify the period within which the information must be provided.[27] Many NCA officers have the operational powers of a police constable, immigration and customs officers, for example, to gain entry to property, conduct searches, seize goods or detain and arrest suspects with or without a warrant.[28]

Criminal prosecutors have powers to require the provision of information. The Director of Public Prosecutions in England and Wales, the Lord Advocate in Scotland and the Director of Public Prosecutions for Northern Ireland (collectively, the Prosecutors) may authorise a specified officer to issue disclosure notices in investigations into offences established in sanctions regulations promulgated under SAMLA.[29] These may require the addressee to answer

21 Her Majesty's Revenue and Customs [HMRC] is primarily responsible for the investigation and enforcement of trade sanctions.

22 See Chapter 9.

23 See section titled 'To whom else to report', below.

24 See https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/bribery-corruption-and-sanctions-evasion.

25 The CPS Specialist Fraud Division has experience in prosecuting trade sanctions and export control cases following HMRC investigations: see https://www.cps.gov.uk/specialist-fraud-division.

26 The power of the Director of the SFO to accept cases for investigation and prosecution is limited to those of serious or complex fraud, or bribery and corruption (CJA 1987, ss 1(3) and 2A(5)). See footnotes 107, 140 and 141, below, for details of the Mabey & Johnson case.

27 OFSI Financial Sanctions Guidance, § 5.6. If no period is specified, compliance must take place 'within a reasonable time'. (See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, reg. 104(1)(a).) As set out above (in the section titled 'Secondary offences') failure to comply with a request for information without a reasonable excuse is a criminal offence, as is providing false information, destroying documentation or otherwise intentionally obstructing OFSI.

28 Crime and Courts Act 2013 s 10, sched. 5.

29 SAMLA s 17(8), amending SOCPA s 61. The Prosecutors' powers are contained within SOCPA s 60. The specified officers are a constable, a designated National Crime Agency [NCA] officer or an HMRC officer.

questions, provide information or produce documents relevant to the investigation.[30] The Director of the SFO can issue 'Section 2 notices', requiring persons under investigation and any other person that the Director has reason to believe has relevant information to answer questions or provide documents 'in any case in which it appears to [the Director] that there is a good reason to do so for the purpose of investigating'.[31] In both cases, the Prosecutors or the Director of the SFO may apply to a court for a warrant to enter and search premises to seize documents in cases where, for example, giving notice for the production of documents might seriously prejudice the investigation.[32]

Civil or criminal investigations

In most cases, the investigation will gather evidence that would be admissible in criminal proceedings. A decision will be taken subsequently whether OFSI will use its civil enforcement powers (whether by monetary penalty or some other action) or will refer the case, usually to the CPS, for criminal prosecution.[33] Since OFSI does not have the power to instigate criminal proceedings of its own accord, if it does refer a case for criminal prosecution, it is a matter for the prosecuting authority to determine whether the case should proceed in accordance with its policy.[34]

Best practice for corporates in an investigation

Once a company becomes aware of a suspected sanctions breach, it should quickly decide on its response strategy. Enforcement authorities place considerable emphasis on timely voluntary disclosure, the extent of a company's cooperation during an investigation and the remedial actions it puts in place to prevent future sanctions violations when deciding the nature and scope of any enforcement action.[35] Companies may also be subject to industry regulatory regimes and shareholder or other disclosure requirements. Companies with operations overseas will need to consider whether regulators in those jurisdictions would expect to be informed.

Actions and issues to be considered after the discovery of suspected breaches or during a sanctions investigation include:

30 SOCPA, s 62(3). They may only be issued when, among other things, the relevant prosecutor has reasonable grounds for (1) suspecting a specified offence has been committed, (2) suspecting that the target has information that relates to a matter relevant to the investigation of that suspected offence, and (3) believing that the information sought is likely to be of substantial value to that investigation.

31 CJA 1987 s 2(1).

32 SOCPA s 66(2); CJA 1987 s 2(4).

33 The distinction between a civil or criminal investigation may only be relevant when the enforcement authority forms an early view that criminal proceedings against any person are unlikely.

34 Note that: 'OFSI will work closely with law enforcement agencies to ensure that breaches of financial sanctions are dealt with in the most appropriate way. We will seek to reach agreement with them where possible, but recognise that sometimes an independent prosecutor may choose not to take forward a prosecution. The 2017 Act also provides additional options for prosecutors when dealing with financial sanctions breaches.' (OFSI Consultation Response on the Process for Imposing Monetary Penalties for Breaches of Financial Sanctions, April 2017, § 1.13.)

35 OFSI Financial Sanctions Guidance, § 7.1; Director of Public Prosecutions and SFO Joint Guidance on Corporate Prosecutions at p. 8.

- notifying the board of directors;
- the board of directors' role going forward and protocol for board communications;
- the role of in-house lawyers and the compliance function;
- appointing external counsel (and other consultants and experts);
- preserving all relevant material (e.g., documents, emails, telephone recordings) concerning both the suspected breaches and the response to their discovery;
- an internal investigation into the suspected breaches;
- reviewing other business and transactions for additional breaches;
- identifying remedial compliance measures;
- early engagement with relevant law enforcement authorities;[36]
- disclosure to other parties (e.g., regulators, shareholders, lenders, insurers, auditors, overseas authorities);
- public relations strategy;
- accounting provision for any anticipated financial penalties and associated costs; and
- disciplinary action against specific employees.

Self-reporting

Overview

In its first financial year (2017–2018), OFSI received 122 reports of suspected breaches of financial sanctions with a reported value of around £1.35 billion.[37] In its second financial year (2018–2019), OFSI received 99 reports of suspected breaches with a reported value of £262 million.[38] In its third financial year (2019–2020), OFSI received 140 reports of suspected breaches with an estimated value of £982.34 million.[39]

The ability of sanctions authorities to perform their monitoring and enforcement roles depends, in large part, on the provision of information about potential sanctions violations by those within the private sector. Therefore, the UK sanctions framework both imposes reporting requirements on certain persons and rewards voluntary disclosure of suspected sanctions breaches.

Self-reporting should be considered by all putative defendants. It is a significant mitigating factor when enforcement authorities decide what action, if any, to take in relation to a sanctions breach and the extent of any penalties.[40] To qualify as 'self-reporting', individuals

36 For example, the Deferred Prosecution Agreements Code of Conduct identifies as a factor that a prosecutor may take into account when deciding whether to enter into a deferred prosecution agreement [DPA], the extent to which the company involves the prosecutor in the early stages of an internal investigation thereby giving the prosecutor the opportunity to give direction as to its scope and the manner in which it is conducted. CPS/SFO Deferred Prosecution Agreements Code of Practice (11 February 2014) [DPA Code] § 2.9.2.

37 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746207/OFSI_Annual_Review_2017-18.pdf.

38 See https://ofsi.blog.gov.uk/2019/10/15/ofsi-releases-2018-to-2019-annual-review/.

39 See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925548/OFSI_Annual_Review_2019_to_2020.pdf.

40 OFSI Monetary Penalties for Breaches of Financial Sanctions [Monetary Penalties Guidance], § 3.28: 'OFSI values voluntary disclosure. Voluntary disclosure of a breach of financial sanctions by a person who has committed a breach may be a mitigating factor when we assess the case. It may also have an impact

or entities cannot rely on self-reporting by another party involved in the suspected breach. If multiple parties are involved, OFSI expects voluntary disclosure from each.[41]

OFSI requires disclosures to include 'all evidence relating to all the facts of the breach'.[42]

Considerations before self-reporting[43]

Whether to self-report

If a person has a legal duty to report to OFSI, failure to self-report is a criminal offence. OFSI, the CPS and the SFO identify in their respective guidance the potential weight they will attach to a genuine self-report as a mitigating factor in all their case disposal decisions.

When to self-report

OFSI expects suspected sanctions breaches to be reported reasonably promptly.[44] It recognises that it may be reasonable for a person to take 'some time' to assess the nature and extent of the breach or to seek legal advice but emphasises that this should not delay an effective response.[45] In the *Standard Chartered Bank* case, OFSI accepted that it was reasonable for the company to report initially the existence of a potential breach and then to provide further information in stages during its internal investigation.[46]

Delaying a self-report risks the law enforcement authority (1) receiving prior notification of the breach from a third party, or (2) concluding that the delay has been unreasonably lengthy, with the result that it will not be a factor weighing against prosecution, in favour of entering into a deferred prosecution agreement (DPA), or justifying a civil penalty discount. If a breach was only discovered as a result of a separate regulatory or law enforcement investigation, the enforcement authority could, potentially, be persuaded that the reporting party should retain the mitigation benefit of voluntary disclosure if it can demonstrate that it quickly instigated a wide-ranging and thorough review of sanctions compliance, cooperated with any external investigation and implemented meaningful remedial actions.[47]

---

on any subsequent decision to apply a penalty.' For further discussion, see section titled 'Civil monetary penalties', below.

41 OFSI Monetary Penalties Guidance, § 3.29.

42 id., at § 3.33.

43 In addition to the actions and issues listed above, in section titled 'Best practice for corporates in an investigation'.

44 OFSI Monetary Penalties Guidance, § 3.32: disclosure should occur 'as soon as reasonably practicable after discovery of the breach' and 'what this means will differ in each case'. See also CPS/SFO Corporate Prosecutions: 'Failure to report wrongdoing within reasonable time of the offending coming to light' is an additional public interest factor in favour of prosecution and self-reporting is an additional public interest factor against prosecution; and CPS/SFO DPA Code §§ 2.8.1(v), 2.9.2 and 2.9.3.

45 OFSI's position is that it is reasonable for a person to take 'some time' to assess the nature and extent of the breach or to seek legal advice, but that doing so should not delay an effective response (OFSI Monetary Penalties Guidance, § 3.32).

46 If there is good reason for delaying the reporting of a breach or for providing partial disclosure, OFSI is able to receive and consider representations (OFSI Monetary Penalties Guidance, § 3.36). For a description of the *Standard Chartered Bank* case, see footnote 138, below.

47 See, e.g., although it was not a sanctions case, *SFO v. Rolls-Royce Plc, Rolls-Royce Energy Systems Inc* [2017] 1WLUK 189, [19] to [22]; see also https://www.sfo.gov.uk/cases/rolls-royce-plc/.

How to self-report

OFSI and the SFO provide information about how to make a report on their respective websites. In both cases, there is a form to be completed and electronically submitted. In practice, an accompanying letter may set out greater detail than is contained within the standard form. The consequences of making an inaccurate disclosure or a disclosure that omits important information can be severe.[48]

To whom else to self-report

Companies should consider whether disclosure should also be made to other domestic regulators or to sanctions authorities in other jurisdictions. This latter point is particularly important if an entity operates in multiple jurisdictions or the breaches took place outside the United Kingdom, since enforcement action in the UK may trigger corresponding investigations overseas and vice versa.[49]

Where the suspected conduct would be in breach only of a non-UK sanctions regime, companies and relevant individuals should still consider whether there are relevant UK regulators to whom a report should be made.[50] Such violations can be indicative of wider institutional control failures even though there has been no breach of applicable UK sanctions. UK anti-money laundering supervisors would expect to be informed of such situations by those they regulate.[51]

Those regulated persons are obliged to make a SAR to the NCA under the UK's anti-money laundering (AML) legislation if they have reasonable grounds to suspect assets are the proceeds of crime. This obligation may be engaged when they suspect sanctions breaches have occurred.[52] Breaches of financial sanctions may also amount to or be linked to other criminal offending, such as the funding of terrorism or bribery and corruption. In such cases, individuals and corporations may have obligations to report information to the police under Section 19 of the Terrorism Act 2000, or reporting obligations under the Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019 or the Anti-Terrorism, Crime

48 'OFSI takes very seriously any evidence that a disclosure did not include relevant information, unless this was a mistake or new facts emerge.' (OFSI Monetary Penalties Guidance, § 3.34).

49 Pre-SAMLA UK sanctions regulations typically included provisions empowering HM Treasury to disclose any information obtained under sanctions regulations to any person for the purpose of facilitating or ensuring compliance with corresponding EU sanctions regulations. This power is extended under SAMLA promulgated regulations to allow disclosure of information to, among other parties, the government of any country. See, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019/411, reg. 108(3)(i). In his introductory remarks following his appointment as Director of OFSI in February 2021, Giles Thomson expressed an intention for OFSI to work with partners in other jurisdictions: 'The UK will continue to work on sanctions with key partners such as the US and the EU, but also with a wider range of partners . . . Sanctions are generally most effective when implemented multilaterally by as many countries as possible.' See footnote 2 above.

50 Although it is outside the scope of this chapter, it is important to note that overseas investigations and prosecutions may give rise to mutual legal assistance and extradition proceedings in the UK. For example, the US has successfully requested the extradition of individuals wanted for prosecution under US sanctions laws, see *Diri v. Government of the United States of America* [2015] EWCA 2130 (Admin); *Tappin v. Government of the United States of America* [2012] EWHC 22 (Admin)

51 See section titled 'Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017', below.

52 See section titled 'Suspicious activity reports', below.

and Security Act 2001.[53] In cases of international bribery and corruption, companies may consider it is in their best interests also to self-report to the SFO.

Other notification requirements

Companies may have contractual obligations to notify counterparties of their involvement in sanctions offences, or in suspected criminal conduct or criminal investigations more generally. These types of clauses are often included in insurance policies, loan and other facility agreements, bank covenants and contracts for international trade. When a company is considering notifying third parties, whether voluntarily or as a requirement, it should also consider informing OFSI and any other relevant law enforcement or regulatory agency of its intention to do so. This is to avoid an allegation of breaching the confidentiality of, or even unlawfully prejudicing, a sanctions investigation.

Anti-money laundering

Introduction

In a suspected sanctions breach,[54] two AML questions arise: (1) has a money laundering offence also been committed? and (2) is the suspected sanctions breach evidence of failings in mandatory AML compliance standards? As noted above, shortly after taking up his post in 2021, the new Director of OFSI emphasised the 'large overlap in threats, issues and stakeholders' in financial sanctions and broader economic crime,[55] and it is anticipated that this understanding will inform both sanctions enforcement policy and OFSI's approach to compliance standards.

The UK's AML legislative regime:[56]

- creates three principal money laundering offences, criminalising:
  - 'concealing, disguising, converting, transferring or removing criminal property from the jurisdiction';[57]

53 Under regulation 21 of the Regulations, a relevant firm (as defined in regulation 22) must inform the Treasury as soon as practicable if it knows or has reasonable cause to suspect that a person is a designated person or has committed an offence under Part 3 or r 20 of the Regulations based on information that came to them in the course of their business. Failure to comply is a criminal offence. Prior to 31 December 2019, the relevant reporting obligations were contained in the Terrorist Asset Freezing Act 2010. Section 19 of the 2010 Act applied when a person believes or suspects that someone has committed an offence under the Act (such as money laundering, the possession or use of funds for terrorism or fund raising for the purposes of terrorism) based on information they obtain in the course of their employment, trade, profession or business. When Section 19 applied, the person was required to disclose the information to a constable as soon as is reasonably practicable.

54 A sanctions breach may also lead to criminal confiscation or civil recovery proceedings in respect of assets obtained through the predicate conduct or any subsequent money laundering offence. See section titled 'Asset recovery', below.

55 See footnote 2 above.

56 The principal money laundering legislation is the Proceeds of Crime Act 2002 [POCA] and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692) [MLR], as amended.

57 POCA s 327. Criminal property is defined, widely, in POCA s 340 as property that constitutes or represents a person's benefit from criminal conduct when the alleged offender knows or suspects that it constitutes such a benefit. 'Property' includes all forms of property wherever situated and in whatever form, including money,

  - 'entering into or becoming concerned in an arrangement known or suspected to facilitate by whatever means the acquisition, retention, use or control of criminal property by or on behalf of another person;[58] and
  - 'acquiring, using or possessing criminal property';[59]
- creates 'supplementary'[60] money laundering offences for failing to disclose suspicious transactions,[61] prejudicing an investigation[62] and tipping off;[63] and
- obliges specified private sector entities (e.g., banks and other financial institutions) to establish and maintain appropriate AML policies and procedures.[64]

Money laundering offences

There are three questions that will determine whether a money laundering offence has been committed: (1) What predicate sanctions offence has been committed? (2) Has 'criminal property' been generated as a result of, or in connection with the sanctions offence? (3) Has there been any distinct or subsequent activity in respect of the 'criminal property', such that an offence under Sections 327 to 329 of the Proceeds of Crime Act 2002 (POCA) has been committed?[65]

Fees received as payment for the unauthorised provision of goods or services to a designated person or otherwise in circumstances that constitute a sanctions offence will be criminal property.[66] The subsequent use, transfer to a third party, or disposal of those fees with the requisite *mens rea* would constitute a money laundering offence under the appropriate provision of Sections 327 to 329 of the POCA.[67]

---

real or personal property, things in action, and other tangible or incorporeal property. An individual will have 'obtained' property if he or she acquires an interest in it, including an equitable interest or power in relation to land in England and Wales, or a right (including a right to possession) in relation to property other than land.

58 POCA s 328.

59 POCA s 329. A conviction for any of the principal offences in POCA ss 327, 328 and 329 carries the following maximum penalties: on summary conviction, six months' imprisonment or a fine (or both) and, on indictment, 14 years' imprisonment or a fine (or both).

60 As described in *R v. GH* [2015] 2 Cr App R 12 (SC) at [14].

61 POCA ss 330 and 331. The sentences on summary conviction are six months' imprisonment or a fine (or both), and on indictment, five years' imprisonment or a fine (or both).

62 POCA s 332.

63 POCA s 333A-E.

64 MLR, reg. 19.

65 Those three questions must be addressed separately because the conduct that amounts to a predicate sanctions offence cannot at the same time amount to an offence under POCA ss 327 to 329; *R v. GH* [2015] 2 Cr App R 12 (SC) at [20], per Lord Toulson: '[I]t is a prerequisite of the offences created by sections 327, 328 and 329 that the property alleged to be criminal property should have that quality or status at the time of the alleged [money laundering] offence . . . Criminal property . . . means property obtained as a result of or in connection with criminal activity separate from that which is the subject of the [money laundering] charge itself.'

66 *R v. McDowell* [2015] 2 Cr App R (S) 14 (CA). Separately, having been obtained through criminal conduct, those fees will be liable to confiscation or civil recovery under POCA.

67 In *R (Golfrate Property Management Ltd) v. Southwark Crown Court* [2014] 2 Cr App R 12 at [104] and [105], the Court of Appeal analysed two factual situations in which a designated person outside the UK transfers funds to a person in the UK. In the first, although the transfer may not, without more, constitute a breach of the asset freezing provisions of the relevant sanctions regime, if the designated person retained a property interest in the funds after the transfer, any subsequent unauthorised movement of the funds may constitute a sanctions offence.

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[68]

UK financial sanctions law does not, directly, require the establishment of sanctions policies and procedures.[69] Nevertheless, a sanctions breach may demonstrate a failure to comply with more general AML and counterterrorist financing (CTF) compliance obligations under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR) such as the obligation to conduct ordinary or enhanced customer due diligence or transaction monitoring.[70] Failing to operate adequate compliance systems to address AML and to combat the financing of terrorism is a breach of Regulation 19 of the MLR, that is to say the requirement under the MLR to adopt 'proportionate' systems and controls.[71] This, in turn, constitutes an offence under Regulation 86 of contravening a relevant requirement, which is punishable by an unlimited fine or imprisonment for two years (or both) following conviction on indictment and three months on summary conviction.

In this first situation, any further use, transfer, etc. of the funds could amount to a money laundering offence. In the second situation, the funds are transferred to a person in the UK with the intent of circumventing the relevant sanctions regulations and a sanctions offence would have been committed at that stage. In this second situation, any subsequent possession, use, transfer, etc. of the funds with the requisite *mens rea* would constitute a money laundering offence.

68 The 2017 Regulations (MLR) remain in force in the UK in amended form, following Brexit. See, e.g. Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020/991

69 Following the 2018 Financial Action Task Force Mutual Evaluation Report for the UK, HM Treasury is considering whether new powers or guidance are necessary to enable all anti-money laundering [AML] supervisors to take enforcement action when there are deficiencies in their regulated populations' financial sanctions systems and controls. HM Treasury, Home Office Economic Crime Plan, 2019-2022, Action 17, para. 4.13. The MLR contain scant reference to economic sanctions although Regulation 33 specifies that when assessing whether there is a high risk of money laundering or terrorist financing for the purpose of applying enhanced due diligence measures and enhanced ongoing monitoring, one of the risk factors relevant firms must take into account is whether the customer is resident in a country 'subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations' (reg. 33(6)(a)(ii), (c)(iii)).

70 The MLR's compliance obligations relating to AML and countering the financing of terrorism apply to 'relevant firms', i.e., persons acting in the course of business carried on by them in the United Kingdom who are credit institutions, financial institutions, auditors, insolvency practitioners, external accountants, tax advisers, independent legal professionals, trust or company service providers, estate agents, letting agents, high-value dealers, casinos, art market participants, cryptoasset exchange providers, custodian wallet providers or auction platforms (reg. 8).

71 In considering what is appropriate or proportionate with regard to the size and nature of its business, a relevant firm may take into account any guidance that has been issued by the FCA or issued by any other supervisory authority or appropriate body and approved by HM Treasury. Reference should be made, inter alia, to the guidance published by the FCA, the Joint Money Laundering Steering Group (JMLSG), the Office for Professional Body Anti-Money Laundering Supervision, the Law Society and other sources. In addition to a breach of the MLR, a regulated person may be in breach of general compliance obligations established under its particular regulatory scheme. For example, FCA regulated entities that fail to adopt appropriate policies and procedures for screening and reporting sanctions breaches may be in breach of general FCA compliance obligations and, in particular: 'Principle 3 of the FCA's Principles for Businesses, which requires regulated firms to take reasonable care to organise their affairs responsibly and effectively, with adequate risk management systems; and SYSC 3.2.6 and related provisions contained in the FCA's Senior Management, Arrangements, Systems and Controls Sourcebook (SYSC) that require firms to establish and maintain effective systems and controls to counter the risk that the firm might be used to further financial crime'. See also, FCA, 'Financial crime: a guide for firms. Part 1: A firm's guide to preventing financial crime' (April 2015) ch. 7 pp. 65 to 72.

The Financial Conduct Authority (FCA) recently announced its first criminal prosecution under the MLR against a bank.[72] As an alternative to bringing criminal proceedings, the designated supervisory authorities under the MLR, such as the FCA, HMRC or various professional bodies,[73] may elect to use their powers to impose civil penalties of fines and issue public statements of censure, prohibit individuals from having a management role in 'a named relevant firm or payment service provider', suspend or remove a person's permission to carry on a regulated activity, deny applications for authorisation or registration, or impose other limitations or restrictions on such persons.[74] In March 2021, the FCA had 42 investigations ongoing into firms and individuals.[75]

The civil fines can be sizable.[76]

In 2020, the FCA fined Commerzbank AG £37.8 million for failing to put adequate AML systems and controls in place between October 2012 and 2017. Although these failings were not specific to sanctions controls, the FCA did note that they occurred 'against a background of heightened awareness within Commerzbank . . . following action taken by US regulators in 2015' in relation to sanctions and AML failings, which the bank settled for a total of US$1.452 million

72 The FCA alleges that, over a period of five years, NatWest bank's systems and controls failed to adequately monitor and scrutinise the payment of approximately £365 million into a customer's accounts, of which around £264 million was in cash. The first appearance in the magistrates' court was scheduled for 14 April 2021: https://www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc (accessed 5 May 21).

73 The UK has 25 AML/CTF supervisors appointed by HM Treasury under the MLR. There are three statutory supervisors (FCA, HMRC and Gambling Commission) and 22 professional body accountancy and legal supervisors. For a complete list, see MLR, reg. 7(1)(b), (2) and sched. 1.

74 MLR regs 76 to 78. See also HMRC Guidance 'Civil Measures for money laundering supervision' (updated 9 December 2020), https://www.gov.uk/government/publications/money-laundering-supervision-enforcement-measures/money-laundering-supervision-civil-measures (accessed 5 May 21).

75 'The importance of purposeful anti-money laundering controls': Speech by Mark Steward, Executive Director of Enforcement and Market Oversight, delivered at the AML & ABC Forum 2021. https://www.fca.org.uk/news/speeches/importance-purposeful-anti-money-laundering-controls (accessed 5 May 21)

76 In 2017, the FCA imposed its largest penalty to date, of £163 million, on Deutsche Bank AG for failing to maintain adequate AML controls, finding that the breaches of the MLR obligations also amounted to a breach of Principle 3 and SYSC rules 6.1.1 R and 6.3.1 R (FCA press release 31 January 2017, at https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure); FCA Final Notice, 30 January 2017, at https://www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf. For details of the FCA's action against Commerzbank, see FCA Final Notice 2020 § 2.7, at https://www.fca.org.uk/publication/final-notices/commerzbank-ag-2020.pdf; Commerzbank AG press release of 12 March 2015, at https://www.commerzbank.com/en/hauptnavigation/aktionaere/service/archive/ir-nachrichten_1/2015_2/ir_nachrichten_detail_15_49802.html. For details of the Financial Services Authority [FSA] action against the Royal Bank of Scotland Group, see FSA press release of 3 August 2010, at https://www.fca.org.uk/news/press-releases/fsa-fines-royal-bank-scotland-group-%C2%A356m-uk-sanctions-controls-failings; FSA Final Decision Notice (2 August 2010), at https://webarchive.nationalarchives.gov.uk/20130202120729/http://www.fsa.gov.uk/static/pubs/other/rbs_group.pdf (accessed 22/5/2020). In October 2020, the FCA and PRA fined Goldman Sachs £96.6 million for risk management failures connected to 1Malaysia Development Berhad (1MDB) and its role in three fund raising transactions for 1MDB, see fca.org.uk/news/press-releases/fca-pra-fine-goldman-sachs-international-risk-management-failures-1mdb and the FCA Final Notice, 21 October 2020 at https://www.fca.org.uk/publication/final-notices/gsi-2020.pdf (accessed 5 May 21).

In 2010, the Royal Bank of Scotland Group was fined £5.6 million for failing to have adequate systems and controls in place to prevent breaches of UK financial sanctions, as required under the Money Laundering Regulations 2007.

Enforcement actions for breach of AML compliance requirements have extended to cases in which the sanctions issues have been breaches of US but not EU or UK sanctions law.[77]

In 2019, Standard Chartered Bank was fined £102 million by the FCA for breaches of the MLR 2007, which was part of US$1.1 billion total financial penalties arising from breaches of US sanctions.

AML supervisory bodies will expect their regulated populations to notify them of known or suspected sanctions breaches.[78]

In 2017, the Prudential Regulation Authority [PRA] of the Bank of England imposed a £17.85 million fine on The Bank of Tokyo-Mitsubishi UFJ Ltd [BTMU] and an associated fine of £8.925 million on MUFG Securities EMEA plc (MUS(EMEA)) for failing to be open and cooperative with the PRA in relation to sanctions enforcement action into BTMU by the New York Department of Financial Services.

This £26.78 million in total fines issued to UK Bank of Tokyo-Mitsubishi entities illustrates the importance UK financial regulators place on international financial institutions making them aware of overseas enforcement actions so that they may assess the implications for the systems and controls of UK affiliates.[79]

77 See https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls. In its Decision Notice, the FCA noted that 'inadequate Due Diligence and ongoing monitoring not only exposed SCB to sanctions evasion but also increased the risk of SCB receiving and/or laundering the proceeds of crime': FCA Decision Notice, para. 2.8, at https://www.fca.org.uk/publication/decision-notices/standard-chartered-bank-2019.pdf. In 2012, HSBC Group received a 'requires action' notice in coordination with but separate to the US$1.92 billion financial penalties imposed by US authorities for breaches of US sanctions laws that had highlighted HSBC's AML and sanctions compliance failings (FSA press release, 11 December 2012, 'FSA requires action of the HSBC Group' (FSA/PN/111/2012), at https://www.fca.org.uk/publications/documents/fsa-requires-action-hsbc-group; FSA Notices (and statements re: firms, individuals) 2012 p. 34.)

78 For FCA regulated firms, this is expressed in Principle 11 of the FCA's Principles for Businesses: 'A firm must deal with its regulators in an open and cooperative way, and must disclose to the FCA appropriately anything relating to the firm of which that regulator would reasonably expect notice.'

79 See https://www.bankofengland.co.uk/news/2017/february/pra-imposes-fine-on-the-bank-of-tokyo-mitsubishi-ufj-limited-and-fine-on-mufg-securities-emea-plc. Note: Conversely, in 2019, British Arab Commercial Bank reported to and involved the PRA in its negotiations with the US Treasury's Office of Foreign Assets Control [OFAC] in respect of apparent breaches of US sanctions. This led to the immediate penalty imposed by OFAC being reduced from US$228.4 million to US$4 million with the remainder suspended because the PRA confirmed that enforcement would lead to the bank becoming insolvent.

Suspicious activity reports

POCA imposes reporting obligations on private entities in the regulated sector and creates offences for non-reporting.[80] These arise when a relevant firm knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering when that knowledge came to them in the course of business.[81] Failing to report suspicions of money laundering or terrorist funding to a firm's nominated officer or to file a SAR as soon as practicable may also demonstrate AML compliance failings that amount to a breach of the MLR.[82] Filing a SAR does not absolve a person in the regulated sector of their obligation to report subject assets[83] of designated persons or breaches of sanctions laws to OFSI.[84] Both those in and outside the regulated sector may file SARs. Irrespective of the obligations upon those within the regulated sector to do so, which are described above, regulated and non-regulated entities may wish to file a SAR in respect of assets with which they intend to deal in order to obtain a Defence Against Money Laundering (DAML) from the NCA, in other words, authorisation to deal with the subject assets. SARs are submitted to the NCA

80 The offences under POCA ss 330 and 331 carry a maximum sentence of five years' imprisonment on indictment. Similar provisions are contained within the Terrorism Act 2000 s 21A in relation to knowledge or suspicion of terrorist financing offences.

81 The threshold of 'suspicion' engaging the requirement to make a SAR is low. In Da Silva [2006] EWCA Crim 1654, [16] and [17], 'suspecting' means the person 'must think there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice'. In an appropriate case, the suspicion 'must be of a settled nature; a case might, for example, arise in which a defendant did entertain a suspicion in the above sense 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'. The test expressed in Da Silva is widely replicated in statutory guidance. See, e.g., the Law Society guide on 'Suspicious Activity Reports', last updated 24 August 2020, at https://www.lawsociety.org.uk/en/topics/anti-money-laundering/suspicious-activity-reports. The JMLSG Guidance describes suspicion (at [6.11]) as 'more subjective [than knowledge] and falls short of proof based on firm evidence. [It is] beyond mere speculation and based on some foundation' – see JMLSG 'Prevention of money laundering/combating terrorist financing' (amended July 2020), see https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-I_-July-2020.pdf.
In deciding whether a person has committed an offence under s 330 or s 331, the court must consider whether he or she followed any relevant guidance which was at the time concerned issued by a supervisory authority or any other appropriate body, approved by the Treasury, and published in a manner it approved as appropriate in its opinion to bring the guidance to the attention of persons likely to be affected by it (POCA s 330(8), s 331(7)). A person does not commit an offence under either of these sections if they have a reasonable excuse for not making the required disclosure or the information that otherwise is required to be disclosed came to the person in legally privileged circumstances (s 330(6)(a), (b)(7B); s 331(6)). A person will not commit an offence under s 330 on the basis that they had reasonable grounds to know or suspect another person is engaged in money laundering where they have not been specified training by their employer. The scope of the 'reasonable excuse' defence is not defined in POCA; it is covered in some of the statutory guidance – see, e.g., The Law Society guide on 'Suspicious activity reports', last updated 24 August 2020, at https://www.lawsociety.org.uk/en/topics/anti-money-laundering/suspicious-activity-reports (accessed 5 May 21).

82 MLR reg. 19(4)(d); see also regs 21(5), 24, 31(1)(d).

83 See POCA ss 335, 338.

84 OFSI, HM Treasury 'UK Financial Sanctions, General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (December 2020) [5.7], see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf (accessed 5 May 21).

via the NCA SAR Online System. The offences under POCA Sections 330 and 331 carry a maximum sentence.[85]

Once a SAR has been filed, POCA prohibits the carrying out of any transaction in relation to the subject property without NCA consent, or the expiry of the prescribed time limits.[86] A person in the regulated sector may not disclose that a SAR has been filed or that a related investigation is being contemplated or is being carried out.[87] A disclosure that is 'likely to prejudice' an investigation amounts to a tipping off offence.[88] Even if no SAR has been filed, if a person knows or suspects that a confiscation investigation, a civil recovery investigation or a money laundering investigation is being or about to be conducted, that person commits an offence by making a disclosure that is likely to prejudice the investigation.[89] This offence is not limited to persons in the regulated sector.[90]

Effect on investigations

The filing of a SAR may be the precursor to a range of investigative orders or civil or criminal asset recovery orders on the application of law enforcement authorities such as the NCA, the police, SFO, HMRC and FCA. These may include:

Crown Court production orders,[91] search warrants,[92] restraint orders[93] and, in post-conviction cases, confiscation orders;[94]

85 The NCA SAR Online System at https://www.ukciu.gov.uk/(hsacnc55jt4f20ucgkvemfbd)/saronline.aspx. The NCA's 2019 annual report records that 478,437 SARs were made in 2018–2019 (NCA, UK Financial Intelligence Unit, Suspicious Activity Reports Annual Report 2019, at https://www.nationalcrimeagency.gov.uk/who-we-are/publications/390-sars-annual-report-2019/file). In 2019–2020, the figure was 573,085 SARs, see nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file (accessed 5 May 21).

86 See POCA ss 335 and 336D. In summary: after an initial period of seven working days, the NCA must either consent to transactions or expressly withhold consent, in which case a moratorium period of 31 days starts to run (s 335). If the NCA does not respond within the initial period, consent is deemed and dealing with the assets would not constitute an offence under ss 330 and 331. If it withholds consent, the NCA may apply to the Crown Court to extend the first moratorium period (the 31 days) for a further (maximum) period of 186 days (s 336A). Only in exceptional circumstances might an account holder be able to seek interim relief requiring a reporting bank to operate an account subject to a SAR during a moratorium period. *National Crime Agency v. N* [2017] 1 WLR 3938.

87 Section 333B protects, subject to conditions, disclosure within the 'undertaking or group', e.g., internally within the bank or internally within a law firm. Sections 333C and 333D protect disclosure in other defined circumstances.

88 POCA s 333A.

89 POCA s 342(2)(a).

90 These provisions do not mean that a SAR may never be disclosed to an account holder but the circumstances in which it will be lawful to do so are limited. *Lonsdale v. National Westminster Bank Plc* [2018] EWHC 1843 (QB).

91 See, e.g., *Golfrate* [2014] 2 Cr App R 12 (money laundering investigation in relation to suspected breach of EU sanctions imposed against members of Zanu-PF precipitated by a bank filing a SAR).

92 In *Golfrate*, the police applied for search warrants under POCA ss 352(1) and 352(6)(b).

93 POCA s 40. A restraint order may be granted if a criminal investigation has begun, there are reasonable grounds to suspect the subject of the restraint order has benefited from his or her criminal conduct, and there is a real risk that the assets will be dissipated if the restraint order is not made.

94 See section titled 'Asset recovery', below.

magistrates' courts' arrest warrants,[95] search warrants,[96] and bank and building society account freezing and forfeiture orders;[97] and

High Court property freezing orders, civil recovery orders[98] and unexplained wealth orders.[99]

Duties of counsel and privilege

Overview

The role of lawyers in sanctions and AML regimes requires special consideration. The starting point is that LPP applies.[100] A professional legal adviser continues to be exempt from the reporting obligations (and related offences) under sanctions legislation and POCA if the information or other matter comes to him or her in legally privileged circumstances.[101]

OFSI recognises that LPP may constitute a reasonable excuse for not disclosing information or documents when otherwise required under sanctions regulations.[102] OFSI's Guidance on Financial Sanctions notes that it 'expects legal professionals to carefully ascertain whether legal privilege applies, and which information it applies to' and observes that OFSI may challenge blanket assertions of privilege.[103]

English law does not distinguish between in-house and independent external counsel for the purposes of LPP.[104] LPP is subject to the 'fraud exception': it does not apply to information or any other matter that is communicated or given to the professional legal adviser with the intention of furthering a criminal purpose.[105]

---

95 Magistrates' Courts Act 1980, s 1.

96 The Police and Criminal Evidence Act 1984 (1984), s 8.

97 POCA, ss 303Z1-8 (freezing) and 303Z14-17 (forfeiture). See footnote 140, below.

98 See, e.g., the Mabey & Johnson case, described in footnotes 114, 150 and 151, below.

99 A requirement for making an unexplained wealth order is that the respondent is either a politically exposed person or there are reasonable grounds for suspecting that the respondent or a person connected with the respondent is or has been involved in serious crime (POCA s 362B(4)). 'Serious crime' includes an offence under UK sanctions legislation (POCA s 362B(9)(a), Serious Crime Act 2007 s 2, Sched. 1 para. 13B).

100 See *Bowman v. Fels* [2005] 1 WLR 3083, 3108F-H, at [78]. For recent Court of Appeal cases considering the scope of the two limbs of LPP, namely litigation privilege and legal advice privilege, see, respectively, *Director of the Serious Fraud Office v. Eurasian Natural Resources Corporation Ltd* [2019] 1 WLR 791 and *R (on the application of Jet2.com Limited) v. Civil Aviation Authority* [2020] EWCA Civ 35.

101 Typical wording for this exclusion in sanctions regulations is contained in, e.g., Democratic People's Republic of Korea (Sanctions) (EU Exit) Regulations 2019, s 109(3): 'Nothing in this Part is to be read as requiring a person who has acted or is acting as counsel or solicitor for any person to disclose any privileged information in their possession in that capacity.' In POCA, see s 330(6) and (7B).

102 'Such protections may apply even where not explicitly referenced' [in the Regulations]. OFSI Monetary Penalties Guidance, [3.38].

103 OFSI, HM Treasury 'UK Financial Sanctions, General guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018' (December 2020) [5.4], see https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/961516/General_Guidance_-_UK_Financial_Sanctions.pdf (accessed 5 May 21).

104 The English law approach is not reflected in EU law: Case C-550/07P, *Akzo Nobel Chemicals Ltd v. Commission of the European Communities* [2011] 2 AC 338.

105 *R v. Central Criminal Court, Ex parte Francis & Francis* [1989] AC 346, 397 (HL): 'privilege will only be excluded in so far as it relates to communications . . . made with the . . . intention of furthering a criminal

Resolution

Overview

OFSI has the power to respond to breaches of financial sanctions by taking action with increasing levels of severity, ranging from low-level outcomes such as issuing a warning, to imposing a civil financial penalty or, in the most serious cases, referring the case for criminal investigation and prosecution.[106] Criminal prosecutions can only be brought where a prosecutor has determined that the proceedings would meet the 'full code test', namely that in respect of each defendant, there is sufficient evidence to provide a realistic prospect of conviction on each charge and that the prosecution would be in the public interest. In contrast, OFSI applies a civil standard to its enforcement actions.

This section starts with an overview of criminal proceedings relating to sanctions offences, including prosecution, DPAs and agreements that individuals may reach with prosecutors. It then describes OFSI's civil penalty regime. It concludes by identifying some of the ancillary measures that may be imposed following a sanctions violation.

Criminal prosecution

Primary sanctions offences and licensing offences are punishable upon conviction on indictment by a fine or imprisonment for up to 10 years.[107] Reporting and information offences are summary offences punishable by a fine or the maximum term of imprisonment that magistrates' courts can impose (six months).[108] Confidentiality offences may be punishable following conviction on indictment by a fine or up to two years' imprisonment.[109]

To secure a conviction, the prosecution must prove beyond reasonable doubt that the person has committed the *actus reus* (conduct) with the requisite *mens rea* (mental element) of the relevant sanctions offence, whether as a principal, a secondary party or as a conspirator. As described above, both companies and corporate officers may be liable for criminal offences.[110]

Historically, UK financial sanctions enforcement by way of criminal prosecution has been limited.[111] Two groups of prosecutions, the *Mabey & Johnson* and *Weir Group* cases, concerned bribes paid in the context of the UN Iraq Oil-For-Food programme.[112]

---

purpose. No other communication will be excluded from the application of the privilege; and the client's confidence will to that extent be protected'. POCA s 330(11) reflects this exception.

106 OFSI Monetary Penalties Guidance, [3.2]. The actions are not mutually exclusive, and several can be taken in a given case. In its 2018–2019 Annual Review, OFSI stated that 'we take some form of action in every instance of non-compliance proportionate to the facts of the case' – see https://ofsi.blog.gov.uk/2019/10/15/ofsi-releases-2018-to-2019-annual-review/.

107 SAMLA s 17(5)(a).

108 This may rise to a maximum term of imprisonment of 12 months for offences committed after s 224 of the Sentencing Act 2020 comes into force. SAMLA s 17(5)(b)(i); see, e.g. Burma (Sanctions) (EU Exit) Regulations 2019/136, reg. 51(4).

109 See, e.g., Burma (Sanctions) (EU Exit) Regulations 2019/136, reg. 51(3).

110 See section titled 'Liability for secondary parties, inchoate offences, corporates and company officers', above.

111 For discussion of prosecutions for breaches of trade sanctions and export controls, see Chapters 8 and 9.

112 The case against the three senior executives of Mabey & Johnson Ltd was subject to interlocutory appellate proceedings: see *R v. Forsyth* [2011] 2 AC 69. The parent company was later subject to High Court civil recovery proceedings. (See footnote 150, below.) For details of the prosecution of Weir Group Plc, see https://www.copfs.gov.uk/publications/bribery-act (accessed 5 May 21).

In 2009, Mabey & Johnson Ltd pleaded guilty to charges including 'making funds available' in violation of Article 3 of the Iraq (United Nations Sanctions) Order 2000. The company was sentenced to total financial penalties, including costs, confiscation, reparations and monitoring costs, of about £6.6 million. Two ex-directors of the company were subsequently tried and convicted for their roles and were sentenced to terms of immediate imprisonment. An ex-sales manager cooperated with the SFO, pleaded guilty and gave evidence against the directors at their trial; he was sentenced to a suspended term of imprisonment.

In 2010, Scottish company Weir Group plc pleaded guilty to breaching sanctions in relation to Iraq through the payment of kickbacks in return for contracts from Saddam Hussein's government. It was sentenced to financial penalties of £3 million and received a confiscation order for £13.9 million.

Deferred prosecution agreements

DPAs are a mechanism by which organisations (typically companies) make an agreement with either the CPS or SFO, under the supervision of a judge, that a criminal prosecution will be suspended for a defined period if the organisation meets certain conditions, which may include financial penalties, compensation, cooperation in the prosecution of individuals and the implementation of appropriate compliance programmes.[113] Since 2017, DPAs have been available in respect of sanctions offences.[114] There has been a small number of DPAs since they were introduced in 2013, most of which have related to significant corporate offending.[115]

The financial penalty levied upon the defendant company must be broadly comparable to the fine that a court would have imposed following conviction after a guilty plea.[116] The non-prosecution, however, may enable the company to avoid significant, consequential financial effects that might flow from a conviction. Airbus, for example, assessed the loss of global revenue that might follow from debarment from public tendering as US$200 billion.[117]

The CPS and SFO DPA Code of Practice governs, among other things, the factors the prosecutor may take into account when deciding whether to enter into a DPA, the process for negotiations, terms of a DPA, including the financial penalty, applying for court approval of a

113 Crime and Courts Act [CCA] 2013, s 45 and sched. 17. The Act identifies the designated prosecutors that may enter into a deferred prosecution agreement [DPA] as the Director of Public Prosecutions in England and Wales [DPP] and the Director of the SFO and any other prosecutor so designated by the Secretary of State (sched. 17 para. 3).

114 CCA 2013 sched. 17 para. 26A, introduced by the Policing and Crime Act [PCA] 2017 s150 and subsequently amended to include sanctions offences created by regulations promulgated under SAMLA.

115 See *R v. Airbus SE* [2020] 1 WLUK 435; *SFO v. Rolls-Royce Plc, Rolls-Royce Energy Systems Inc* [2017] 1 WLUK 189; *Tesco Stores Ltd* [2017] 4 WLUK 558; *SFO v. XYZ Limited* (unrep) 11 July 2016, Sir Brian Leveson P; *SFO v. Standard Bank Plc* [2015] 11 WLUK 802.

116 CCA 2013 sched. 17 para. 5(4); SFO/CPS DPA Code of Practice §§ 7.9(iii), (iv), 8.3, 8.4; Standard Bank Plc [2015] 11 WLUK 804, [16].

117 *Director of the Serious Fraud Office v. Airbus SE* [2020] 1 WLUK 435 [85].

DPA and overseeing a DPA after its approval.[118] Voluntary self-reporting, subsequent cooperation and restorative measures are public interest factors tending away from prosecution and towards a DPA.[119] The DPA Code will apply in sanctions breach cases, as will the Code for Crown Prosecutors, the CPS/SFO Joint Prosecution Guidance on Corporate Prosecutions and, where corruption offences may also have occurred, the Joint Prosecution Guidance on the Bribery Act 2010.

Arrangements between prosecutors and individual defendants

Frequently there are plea arrangements between defendants and prosecutors, which may take various forms. In some, the defendant pleads guilty to part of an indictment and the prosecution offers no evidence on the remaining counts on that indictment or asks the court to allow those counts to lie on the file. In others, the defendant pleads guilty to a lesser offence or to the indicted offence but on a less serious factual basis than that originally alleged against them.[120]

When a defendant offers to provide information or to give evidence about the criminal activities of others, they may enter into a formal written arrangement with a specified prosecutor known as a 'SOCPA agreement'.[121] In return for providing information or giving evidence in accordance with the agreement, a defendant could potentially achieve immunity from prosecution[122] but more likely would receive a reduced sentence in respect of his or her own criminality.[123] The level of sentence reduction will depend on the timing, nature, extent and value of the assistance offered or provided. In cases of genuine and substantial assistance, it could be a reduction of between one-half and two-thirds of the sentence that a defendant would otherwise receive.[124]

Civil monetary penalties

Following the establishment of OFSI in 2016, HM Treasury was given a power to impose monetary penalties for sanctions breaches on companies and officers of companies.[125] It may impose a monetary penalty if satisfied, on the balance of probabilities, that a person has breached a prohibition or failed to comply with an obligation imposed by or under financial

118 See https://www.cps.gov.uk/sites/default/files/documents/publications/dpa_cop.pdf.

119 DPA Code of Practice § 2, in particular § 2.8.1(iii), (iv), (v), § 2.8.2(i), §2.9.1.

120 The principles an English prosecutor should apply in these situations are contained within Section 9 of the Code for Crown Prosecutors and the Attorney-General's Guidelines on the Acceptance of Pleas and the Prosecutor's Role in the Sentencing Exercise. Additionally, the Attorney-General's Guidelines on Plea Discussions in Cases of Serious or Complex Fraud may apply in some sanctions cases.

121 SOCPA ss 71 to 75B. See also, CPS guidance 'SOCPA 2005 – Queen's evidence: Immunities, Undertakings and Agreements' and 'SOCPA Agreements: Note for those representing assisting offenders'. The DPP and the Director of the SFO are specified prosecutors: SOCPA s 71.

122 SOCPA s 71 empowers a specified prosecutor to issue a written immunity notice with the effect that no proceedings for any offence specified in the notice may be brought against that person except in circumstances specified in the notice. An immunity notice ceases to have effect if the person fails to comply with any conditions specified within it.

123 For a 'typical example' of such an agreement, see *Blackburn* [2008] 2 Cr App R (S) 5, [7].

124 *Blackburn* [2008] 2 Cr App R (S) 5, [41].

125 PCA 2017 ss 146 to 149.

sanctions legislation and that the person knew or had reasonable cause to suspect that he or she was in breach of the prohibition or had failed to comply with the obligation.[126] When a monetary penalty is payable by a legal person, HM Treasury may also impose a monetary penalty on an officer of the body if satisfied, on the balance of probabilities, that the legal person's breach or failure took place with the consent or connivance of the officer or was attributable to any neglect by the officer.[127] If OFSI can estimate the value of the funds involved in the breach, the maximum penalty is the greater of £1 million or 50 per cent of the estimated value. In all other cases, the maximum penalty is £1 million.[128]

OFSI must observe various procedural steps before imposing a monetary penalty. They include providing the target with (1) notice of OFSI's intention to impose a monetary penalty;[129] (2) an opportunity to make representations about any relevant matters, including matters of law, the facts of the case, how OFSI has followed its process and whether the penalty is fair and proportionate;[130] and, if a penalty is imposed, (3) the right to a ministerial review.[131] There is then a right of appeal to the Upper Tribunal.[132]

When deciding how to dispose of a case and the size of any monetary penalty, OFSI applies a three-step process: (1) penalty threshold; (2) baseline penalty matrix; and (3) penalty recommendation.[133] The penalty threshold is met if the statutory threshold for imposing a penalty has been met and a monetary penalty would be appropriate and proportionate. The 'appropriate and proportionate' limb will most likely be met if (1) funds or economic resources were made available to a designated person, (2) the sanctions prohibitions were circumvented, or (3) there was non-compliance with a requirement to provide information.[134] If none of these factors is present, OFSI may still conclude that a monetary penalty is appropriate and proportionate.[135]

A 'baseline penalty matrix' is used to calculate the appropriate penalty. First, OFSI will calculate the statutory maximum: the greater of £1 million or 50 per cent of the breach. Second, it will identify a 'reasonable and proportionate' penalty based on its view of the seriousness of the case. This is the 'baseline penalty level'. This could be any amount between the maximum and zero. Third, it will consider whether a penalty reduction for 'prompt and complete voluntary disclosure of the breach' is warranted. In 'serious' cases, this reduction can

126 id., at s 146(1).

127 id., at s 148.

128 id., at s 146(3).

129 OFSI Monetary Penalties Guidance, § 5.2

130 id., at § 5.4.

131 id., at § 6.3. PCA 2017 at s 174. These are reflected in OFSI's Monetary Penalties Guidance. OFSI will impose a 28-day period in which to make representations. Late representations are not normally accepted and any request for an extension must be accompanied by evidence (OFSI Monetary Penalties Guidance, § 5.10). If no representations are made within that time frame, the penalty will be finalised and the person will become liable to make payment (§ 5.11). OFSI aims to issue a response within 28 working days of the deadline for representations (§ 5.13).

132 PCA 2017 s 146(6). The Upper Tribunal may quash the Minister's decision and (1) quash the decision to impose a penalty or (2) uphold the decision to impose a penalty but substitute a different amount for the amount determined by HM Treasury (s 146(7)).

133 OFSI Monetary Penalties Guidance, § 4.1.

134 id., at § 4.3.

135 id.

be up to 50 per cent of the baseline penalty. In the 'most serious' cases, the potential reduction is capped at 30 per cent.[136] 'Most serious' cases may involve a very high value; particularly poor, negligent or intentional conduct; or severe or lasting damage to the purposes of the sanctions regime.[137]

OFSI will determine whether a penalty is proportionate based on the relationship between the proposed penalty and a 'holistic assessment' of all the other factors present in the case. Penalties need not be 'a specific percentage or multiple of the breach amount'.[138]

When assessing the seriousness of a case, deciding whether or what type of enforcement action is required and identifying aggravating or mitigating factors to determine an appropriate monetary penalty, OFSI will generally take into account the following:[139]

- the value of the breach;[140]
- harm or risk of harm to the objectives of the sanctions regime;[141]
- whether the breach is deliberate, negligent or the result of an error;[142]
- whether the breach is the result of broader systems failures;
- repeated or persistent breaches;[143]
- voluntary self-disclosure of suspected breaches;[144] and
- the public interest in responding to the breaches.[145]

In 2017 and 2018, OFSI did not impose any civil monetary penalties. Between January 2019 and March 2020, it imposed four monetary penalties, two of which were subject to a ministerial review.[146]

---

136 id., at § 4.8–4.9; § 4.11.

137 id., at § 3.46.

138 id., at § 4.8.

139 OFSI reserves the right to take into account any factor that it considers material and relevant, id., at § 3.42.

140 OFSI Monetary Penalties Guidance, § 3.17. High-value breaches are generally more likely to result in enforcement action.

141 id., at § 3.18.

142 id., at § 3.22-3.23. OFSI may take into account the actual and expected level of knowledge of sanctions law within an organisation or in respect of an individual (OFSI Monetary Penalties Guidance, § 3.19). Failure by regulated professionals to meet regulatory and professional standards may be an aggravating factor. § 3.20.

143 OFSI Monetary Penalties Guidance, § 3.26.

144 See section titled 'Self-reporting', above.

145 OFSI Monetary Penalties Guidance, § 3.39.

146 See https://www.gov.uk/government/collections/enforcement-of-financial-sanctions. The penalties were as follows:
(1) Raphael Bank (January 2019): £5,000 penalty for dealing with funds of £200 belonging to a person designated under the Egypt (Asset-Freezing) Regulations 2011. A 50 per cent reduction for voluntary disclosure was applied.
(2) Travelex (UK) Ltd (March 2019): £10,000 penalty for dealing with the same funds as Raphael Bank, despite having access to the designated person's passport, which clearly identified the individual by name, date of birth and nationality. There was no voluntary disclosure and so no penalty reduction.
(3) Telia Carrier UK Limited (September 2019): £146,341 penalty, reduced from £300,000 following a ministerial review for making economic resources available to a designated person under the Syria sanctions regime by indirectly facilitating international telephone calls to SyriaTel repeatedly and for an extended period. During the review, the value of the breaches was reassessed as approximately £234,000, There was no voluntary disclosure.

In 2020, Standard Chartered Bank received penalties of £20.47 million from OFSI for breaches of Ukraine-related sanctions by granting loans worth £97.5 million to the subsidiary of a designated Russian entity.

Although caution must be exercised in drawing conclusions from this limited pool of cases, the *Standard Chartered Bank* case marks a significant step change and signals a preparedness by OFSI to issue substantial penalties. It also demonstrates the value placed by OFSI on self-reporting, cooperation and remedial action following suspected sanctions breaches. The *Raphael Bank* case suggests that even self-reported breaches of modest value may be considered sufficiently 'serious' for the OFSI to determine that a civil monetary penalty is 'appropriate and proportionate'.

Ancillary orders and additional consequences of sanctions breaches

Asset recovery

Recovery of property obtained as a result of sanctions offences may be pursued through confiscation proceedings following prosecution and conviction[147] or in separate civil proceedings.[148]

There is also the possibility that property frozen under sanctions regulations (which do not themselves alter the legal rights and interests in the property) may itself be subject to an asset recovery order. This could occur where the frozen assets are the realisable property of a convicted person or the property can be shown to have been obtained through or by unlawful conduct, or where a private claimant sought to enforce a judgment debt against the assets. As an example of the latter, in *R (Certain Underwriters at Lloyds) v. HM Treasury* [2021] 1 WLR 387, the claimants sought information from HM Treasury in relation to assets frozen pursuant to sanctions against the Syrian regime as a precursor to applying to HM Treasury for a licence to enforce a US judgment debt against those assets. Looking forward, we anticipate

(4) Standard Chartered Bank (March 2020): £20.47 million total penalties, reduced from £31.5 million following a ministerial review. A 30 per cent reduction for voluntary disclosure was applied. The Minister substituted a lower penalty figure after finding that although it was a 'most serious' case, OFSI had given insufficient weight to facts that Standard Chartered had not wilfully breached the sanctions regulations, acted in good faith, intended to comply with the restrictions, fully cooperated with OFSI and had taken remediation steps. (OFSI Report, 'Imposition of Monetary Penalty – Standard Chartered Bank', [14]).

147 *R v. McDowell* [2015] 2 Cr App R (S) 14 (CA). M had negotiated the sale of prohibited items from China to Ghana without a licence in contravention of Articles 4 and 9(2) of the Trade in Goods (Control) Order 2003. In addition to a sentence of two years' suspended imprisonment, the confiscation order made against M was based on his gross receipts for the trades (approximately £2.5 million) and the commission payments he received.

148 In *Mabey & Johnson*, the offending company's parent company settled civil asset recovery proceedings instituted by the SFO in the High Court under Part 5 of POCA for £130,000 in recognition of sums it had received through share dividends derived from contracts won by Mabey & Johnson Ltd through unlawful conduct: see https://webarchive.nationalarchives.gov.uk/20120314165057/http://www.sfo.gov.uk//press-room/latest-press-releases/press-releases-2012/shareholder-agrees-civil-recovery-by-sfo-in-mabey--johnson.aspx. In 2019, monies received by a niece of Syrian president Bashar al-Assad in breach of the Syrian sanctions regulations were subject to a magistrates' court bank account forfeiture order. David Brown, 'Aniseh Chawkat: Police freeze Assad niece's bank account in London', *The Times*, 22 May 2019, at https://www.thetimes.co.uk/article/aniseh-chawkat-police-freeze-assadniece-s-bank-account-in-london-5qr07sxpl.

that this interplay between property frozen under sanctions regulations and law enforcement asset recovery measures may also emerge.

Monitorships

Monitors are independent third parties, generally law firms, risk consultancies or professional service firms, appointed by the court to oversee and report on a company's internal controls and compliance functions following a criminal or regulatory investigation. A monitor may be appointed voluntarily by a company (e.g., to demonstrate cooperation during an investigation) or agreed between the company and the investigating agency as part of a negotiated settlement and presented for court approval.[149] A monitor may also be appointed under the terms of a DPA[150] or as part of a serious crime prevention order (SCPO)[151] or civil recovery order.[152]

Serious crime prevention orders

SCPOs are designed to prevent, restrict or disrupt involvement in serious crime. They may be made in respect of sanctions offences.[153] SCPOs can be made against natural or legal persons and may, among other things, impose restrictions or requirements in relation to financial, property or business dealings or holdings, and require a person to answer questions or provide information.[154] When a SCPO is made against a legal person (usually a company or a partnership), it can include the appointment of an authorised monitor, paid for by that legal person.[155] SCPOs may be imposed for up to five years.[156]

SCPOs can be made by the Crown Court during sentencing[157] or in separate civil proceedings in which a conviction is not a prerequisite, if the court is satisfied that a person has been involved in serious crime, whether in the United Kingdom or elsewhere, and it has reasonable grounds to believe that the order would protect the public by preventing, restricting or disrupting involvement by the person in serious crime in the relevant part of the UK.[158]

---

149 Following its conviction in 2009 for bribery and breaching UN sanctions against Iraq, Mabey & Johnson Ltd was required to instruct an SFO-approved monitor for up to three years, whose costs for the first year were capped at £250,000.

150 The DPA Code of Practice addresses the potential appointment of compliance monitors. It states that it is important for a prosecutor to consider whether the organisation already has a 'genuinely proactive and effective corporate compliance programme' and that the use of monitors 'should therefore be approached with care'. Ultimately, the guidance explains: 'The appointment of a monitor will depend upon the factual circumstances of each case and must always be fair, reasonable and proportionate.'

151 Serious Crime Act [SCA] 2007, s 39.

152 For a detailed guide to monitorships, see https://globalinvestigationsreview.com/benchmarking/the-guid e-to-monitorships-second-edition/1226581/11-monitorships-in-the-united-kingdom (accessed 5 May 21).

153 PCA 2017 s 151.

154 SCA 2007, s 5(3) to 5(5).

155 id., at s 39.

156 id., at s 16(2). See s 22E for the power to extend orders pending the outcome of criminal proceedings.

157 id., at s 19.

158 id., at s 1. They can be made by the English High Court, an appropriate court in Scotland or the High Court in Northern Ireland on an application by a specified prosecutor, namely, the DPP or the Director of the SFO in England and Wales, the Lord Advocate for an order in Scotland and the DPP for Northern Ireland in the case of an order in Northern Ireland (s 8).

SCPO proceedings in both the Crown Court and the High Court are civil proceedings and the civil standard of proof is applied.[159] Breach of an SCPO without reasonable excuse is a criminal offence punishable with imprisonment for a term not exceeding five years or a fine, or both.[160]

Debarment

A breach of sanctions may result in debarment from tendering for public sector contracts in the United Kingdom and elsewhere.[161] In the UK, tendering for public sector contracts is governed by the Public Contracts Regulations 2015, which implement the EU Procurement Directive.[162] Sanctions breaches may result in discretionary debarment.[163]

Directors' disqualification and regulatory measures

Upon conviction for an offence in connection with, inter alia, the promotion or management of a company, the court may make a disqualification order for up to 15 years.[164] Breach of a disqualification order is a criminal offence.[165]

Even without a conviction, a sanctions breach will be relevant to the FCA's and HMRC's assessment of the continuing 'fitness and propriety' of approved persons and may result in withdrawal of approval.[166]

159 SCA 2007 ss 35 and 36.

160 id., at s 25.

161 See, e.g., Director of the Serious Fraud Office v. Airbus SE [2020] 1 WLUK 435 [84].

162 Amendments to the Regulation will come into force following Brexit.

163 Regulation 57 of the Public Contract Regulations 2015; see also, e.g., Director of the Serious Fraud Office v. Airbus SE [2020] 1 WLUK 435 [84].

164 Company Directors Disqualification Act [CDDA] 1986 s 2.

165 CDDA 1986 ss 13 and 14.

166 See section titled 'Anti-money laundering', above. See also FCA, 'Fit and Proper test for Employees and Senior Personnel sourcebook', at https://www.handbook.fca.org.uk/handbook/FIT.pdf (last accessed 5 May 21) and HMRC, 'The fit and proper test and HMRC approval technical guidance', at https://www.gov.uk/government/publications/money-laundering-supervision-fit-and-proper-test-and-approval/money-laundering-supervision-guidance-on-the-fit-and-proper-test-and-hmrc-approval (updated 15 September 2020) (accessed 5 May 21).

Appendix 2

About the Authors

Rachel Barnes
Three Raymond Buildings

Dr Rachel Barnes is a dual-qualified US attorney and English barrister. She is recognised as a leading practitioner in the area of sanctions, as well as corruption, financial and corporate crime, international crime, extradition and mutual legal assistance, and proceeds of crime and asset recovery.

Rachel has a wealth of sanctions experience as a practitioner, academic and expert witness. She is 'one of the best navigators of the complex financial and trade sanctions regime' (*Chambers* 2018), 'go-to counsel on matters with a transatlantic element' (*Chambers* 2019), 'pragmatic, hands-on, easy to work with, always available' and 'devastatingly well prepared in court' (*Chambers* 2020) and 'the first and last stop for financial sanctions advice' (*Chambers* 2021).

Rachel regularly acts in both domestic and international sanctions cases. As an English barrister, Rachel both prosecutes and defends in criminal cases, and civil and public law crime-related matters. Her clients include governments, corporations, NGOs and individuals. She is prosecuting counsel for the UK's Serious Fraud Office and Financial Conduct Authority and appointed to the Attorney General's specialist panel of public international law counsel. Rachel appears in cases in the Crown Court, the High Court, the Court of Appeal and the UK's Supreme Court, as well as acting for a number of successful petitioners before the UN Ombudsperson. Rachel previously taught law at Cambridge University and the London School of Economics and Political Science.

Saba Naqshbandi
Three Raymond Buildings

Saba Naqshbandi is a leading specialist in commercial crime with a longstanding and recognised reputation. Her areas of expertise include bribery and corruption, fraud, insider dealing, money laundering, cash seizure and forfeiture, confiscation and restraint. In addition to her

trial practice, she has a co-existing high net worth individual and corporate foreign client practice. Given her expertise, Saba is instructed in civil and commercial cases where there is need for a criminal fraud specialist.

She has been recognised in the directories for her 'sharp strategic insight', 'excellent tactical judgement' and for being 'smart and absolutely charming with judges. She focuses judges' minds on the points they need to focus on and is very adept at dealing with clients'.

Patrick Hill
Three Raymond Buildings

Patrick Hill represents and advises companies and individuals in matters relating to asset forfeiture, sanctions, complex fraud, money laundering and regulatory offences. He has acted in applications for delisting to the European Commission, the United Nations Security Council and the UN Ombudsperson.

Genevieve Woods
Three Raymond Buildings

Genevieve Woods has particular expertise in white-collar crime and international sanctions. Genevieve regularly advises on cases involving sanctions violations, including those involving the determination of civil penalties by HM Revenue and Customs, the Office of Financial Sanctions Implementation and the US Treasury's Office of Foreign Assets Control. She has worked on complex sanctions and export control cases for international corporations, including financial institutions, insurance companies and maritime corporations, in large-scale internal investigations and compliance reviews. In addition, she has advised corporations and individuals about the risk of breach in relation to contemplated transactions. Genevieve studied the impact of international sanctions while undertaking a master's in international human rights law at Oxford University and has written articles regarding sanctions enforcement.

Three Raymond Buildings
3 Raymond Buildings
Gray's Inn
London WC1R 5BH
United Kingdom
Tel: +44 20 7400 6400
rachel.barnes@3rblaw.com
saba.naqshbandi@3rblaw.com
patrick.hill@3rblaw.com
genevieve.woods@3rblaw.com
www.3rblaw.com

We live in a new era for sanctions. More states are using them, in more creative (and often unilateral) ways.

This creates ever more complication for everybody else. Hitherto no book has addressed all the issues raised by the proliferation of sanctions regimes and investigations in a structured way. GIR's *The Guide to Sanctions* addresses that. Written by contributors from the small but expanding field of sanctions enforcement, it dissects the topic in a practical fashion, from every stakeholder's perspective, providing an invaluable resource.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-596-2