

International Comparative Legal Guides



Practical cross-border insights into sanctions

Sanctions 2022

Third Edition

Contributing Editors:

Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

ICLG.com



ISBN 978-1-83918-144-3
ISSN 2633-1365

Published by

glg global legal group

59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
info@glgroup.co.uk
www.iclg.com

Publisher
Jon Martin

Production Editor
Hollie Parker

Senior Editor
Sam Friend

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

Printed by
Ashford Colour Press Ltd.

Cover image
www.istockphoto.com

Strategic Partners



International Comparative Legal Guides

Sanctions 2022

Third Edition

Contributing Editors:

Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP

©2021 Global Legal Group Limited.

All rights reserved. Unauthorised reproduction by any means, digital or analogue, in whole or in part, is strictly forbidden.

Disclaimer

This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice. Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.

This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Expert Analysis Chapters

- 1** **Recent Developments in U.S. Sanctions: OFAC Enforcement Trends and Compliance Lessons Learned**
Roberto J. Gonzalez & Rachel M. Fiorill, Paul, Weiss, Rifkind, Wharton & Garrison LLP
- 8** **No End in Sight: An Update on the Rising Risk and Recent Developments in Cryptocurrency Sanctions and Enforcement**
Adam Klauder, Guidehouse
- 17** **The New EU Global Human Rights Sanctions Regime**
Salomé Lemasson, Rahman Ravelli
- 21** **Annual Developments in EU Sanctions Litigation**
Sebastiaan Bennink, Shanne Verkerk & Sarah Reilly, BenninkAmar Advocaten

Q&A Chapters

- 29** **Australia**
Johnson Winter & Slattery: Robert Wyld & Lara Douvartzidis
- 38** **Austria**
Dorda Rechtsanwälte GmbH: Bernhard Müller & Heinrich Kühnert
- 44** **China**
JunHe LLP: Weiyang (David) Tang, Juanqi (Jessica) Cai, Runyu (Roy) Liu & Siyu (Rain) Wang
- 51** **France**
BONIFASSI Avocats: Stéphane Bonifassi & Sinem Paksut
- 57** **Germany**
Gibson, Dunn & Crutcher LLP and EY Forensic & Integrity Services: Michael Walther, Richard Roeder, Meribeth Banaschik & Bisman Sethi
- 67** **Italy**
Delfino e Associati Willkie Farr & Gallagher LLP: Gianluca Cattani & Fabio Cozzi
- 74** **Japan**
Nishimura & Asahi: Kazuho Nakajima, Masahiro Heike & Yumiko Inaoka
- 80** **Korea**
Yulchon LLC: Tong-chan Shin, Jae Hyong Woo & Yong Ju Lee
- 87** **Netherlands**
De Brauw Blackstone Westbroek N.V.: Marlies Heemskerk-de Waard & Marnix Somsen
- 92** **Norway**
Kluge Advokatfirma AS: Ronny Rosenvold & Siri Fosse Sandve
- 99** **Russia**
Rybalkin, Gortsunyan & Partners: Oleg Isaev, Anastasia Konstantinova & Marina Abazyan
- 106** **Sweden**
Advokatfirman Vinge KB: Anders Leissner & Tove Lövgren Frisk
- 111** **Switzerland**
Homburger: Claudio Bazzani & Reto Ferrari-Visca
- 116** **United Arab Emirates**
BSA Ahmad Bin Hezeem & Associates LLP: Rima Mrad & Tala Azar
- 123** **United Kingdom**
HFW: Daniel Martin
- 129** **USA**
Paul, Weiss, Rifkind, Wharton & Garrison LLP: Roberto J. Gonzalez & Rachel M. Fiorill

Preface

Welcome to the third edition of *ICLG – Sanctions*. Paul, Weiss, Rifkind, Wharton & Garrison LLP is delighted to serve as the *Guide’s* Contributing Editors and authors of two chapters.

This edition covers the economic sanctions laws of 16 jurisdictions, and its opening chapters survey key regulatory and enforcement topics. The *Guide* brings together the expertise and perspectives of leading practitioners across the world. It is our belief that the *Guide* will serve as a valuable resource for those seeking to understand sanctions regimes across jurisdictions and a concise primer on the various forms of sanctions, types of sanctions enforcement, and compliance expectations.

Sanctions are increasingly used as an important (and sometimes the primary) tool of foreign policy, and a number of jurisdictions have increased their focus on the enforcement of sanctions requirements. As sanctions continue to expand and change at a rapid pace, those engaged in international trade are forced to navigate an increasingly complex – and sometimes conflicting – regulatory environment. We hope the *Guide* serves as a useful roadmap.

We encourage you to contact us with suggestions for future editions.

Roberto J. Gonzalez & Rachel M. Fiorill
Paul, Weiss, Rifkind, Wharton & Garrison LLP



ICLG.com

Recent Developments in U.S. Sanctions: OFAC Enforcement Trends and Compliance Lessons Learned

Paul, Weiss, Rifkind, Wharton & Garrison LLP



Roberto J. Gonzalez



Rachel M. Fiorill

Introduction

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") is in the midst of a record-setting streak of enforcement. Since January 2020, OFAC has taken 27 public enforcement actions and assessed over \$39.2 million in civil monetary penalties. Increasingly, OFAC has drawn explicit links in its public enforcement actions to the compliance expectations laid out in its landmark 2019 guidance on the "hallmarks of an effective compliance program" (the "Framework"). U.S. and non-U.S. companies alike would be well-served to learn from the mistakes of similarly situated entities and incorporate the compliance guidance found in recent OFAC enforcement actions into their own sanctions risk assessments and compliance programmes.

This chapter discusses several of the main themes from recent OFAC enforcement actions and highlights the related compliance lessons learned.

OFAC's Compliance Framework

The 2019 Framework, and the related "compliance commitments" that are now a standard part of OFAC settlements, represent a new effort by OFAC to more clearly and comprehensively communicate its expectations about appropriate sanctions compliance practices. OFAC made clear that the guidance is intended not only for U.S. companies, but also for non-U.S. companies that conduct business in or with the United States, with U.S. persons, or using U.S.-origin goods or services. U.S. and non-U.S. companies would be well-advised to study the Framework carefully because, among other things, OFAC will consider a compliance programme that follows the Framework, a mitigating factor in the event of an enforcement action.¹

The Framework describes five "essential components" of an effective sanctions compliance programme ("SCP"):²

- **Management Commitment.** The Framework notes that Senior Management's³ commitment to, and support of, a company's risk-based SCP is "one of the most important factors in determining its success". This commitment can be evidenced by management's: (1) review and approval of the SCP; (2) ensuring that the compliance function has sufficient authority and autonomy to deploy policies and procedures to effectively control OFAC risk (this includes the designation of a sanctions compliance officer); (3) ensuring the compliance function receives adequate resources; (4) promoting a "culture of compliance"; and (5) recognition of the seriousness of, and the implementation of necessary measures to reduce the occurrence of, sanctions violations.⁴

- **Risk Assessment.** As is consistent with OFAC's past practice, the Framework recommends that SCPs be designed and updated pursuant to a "risk-based approach". OFAC officials have emphasised that not every company is expected to satisfy every element of the Framework, but rather companies should tailor their programmes to their unique risk profiles. One of the "central tenets" of a risk-based approach is for companies to "conduct a routine, and if appropriate, ongoing 'risk assessment' for the purposes of identifying potential OFAC issues they are likely to encounter."⁵ OFAC identifies two core elements of a commitment to meet this compliance component: periodic risk assessments (including the conducting of due diligence during client and third-party onboarding and merger-and-acquisition activities); and the development of a methodology to analyse and address the particular risks identified by these risk assessments (which could include the root causes of any apparent violations or systemic deficiencies identified by the organisation during the routine course of business as well as through its testing and audit function).⁶
- **Internal Controls.** Effective OFAC compliance programmes generally include internal controls to identify, interdict, escalate, report, and keep records pertaining to prohibited activity. Key elements include: (1) written policies and procedures tailored to the organisation's operations and risk profile and enforced through internal and/or external audits; (2) adequately addressing the results of a company's OFAC risk assessment; (3) implementation of immediate and effective remedial actions; (4) clear communication of policies and procedures to all relevant staff; and (5) identification of designated personnel responsible for integrating policies and procedures into daily operations.⁷
- **Testing and Auditing.** A comprehensive and objective SCP audit function ensures the identification of programme weaknesses and deficiencies. OFAC notes that it is the company's responsibility to enhance its programme, including all programme-related software, systems, and other technology, to remediate any identified compliance gaps.
- **Training.** The Framework describes training as "integral" and outlines OFAC's expectation that training programmes be "provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually) and generally should accomplish the following: (i) provide job-specific knowledge based on need; (ii) communicate the sanctions compliance responsibilities for each employee; and (iii) hold employees accountable for sanctions compliance training through assessments"⁸.

As an appendix to the Framework, OFAC also describes some of the common “root causes” of the violations that were the subject of its prior enforcement actions. These themes and others are addressed in the enforcement trends section below.

Enforcement trends

Consistent with its new focus on compliance, OFAC has routinely incorporated compliance commitments into its public settlement agreements since December 2018; these settlements have involved both financial institutions and non-financial institutions.⁹ In these settlements, OFAC has also imposed a requirement that the settling party annually certify its compliance with the commitments over a five-year period, a process which will likely require settling parties to invest additional resources in their SCPs and therefore increases the costs associated with OFAC settlements.

OFAC’s enforcement actions in 2020 and the first half of 2021, together with the Framework’s discussion of “root causes”, highlight compliance deficiencies or breakdowns that are commonly responsible for sanctions violations. We describe the major areas of concern below.

Use of the U.S. financial system, including the use of U.S. dollar payments

OFAC has long viewed the use of the U.S. financial system for the benefit of sanctioned persons or jurisdictions as constituting a violation of U.S. sanctions.

OFAC’s “big bank” enforcement actions have historically focused on global banks utilising “wire stripping” or other non-transparent payment methods to process transactions prohibited by U.S. sanctions through the U.S. financial system.¹⁰ The 2019 multiagency resolutions with UniCredit Group (“UniCredit”) (\$1.3 billion in combined fines) and Standard Chartered Bank (“SCB”) (\$1.1 billion in combined fines assessed by the United States and United Kingdom), shows that the march of large, multi-agency enforcement actions against banks for such conduct continues to the present day.¹¹ The SCB action demonstrates that U.S. regulators have also taken enforcement action against financial institutions outside the context of “wire stripping” or other non-transparent payment methods. For example, DOJ cited the bank’s transactions with an Iranian national who allegedly used supposed general trading companies in the UAE as fronts for a money exchange business located in Iran, and OFAC highlighted the bank’s alleged delays in restricting sanctioned country access to its online banking platform and fax transmissions as a compliance failure that led to apparent sanctions violations.

Historically, OFAC and DOJ enforcement focused on banks – and not the banks’ customers – that were conducting transactions with sanctioned jurisdictions or parties. However, in 2017, OFAC made clear through its enforcement action against Singaporean entity CSE Global Limited and its subsidiary CSE TransTel Pte. Ltd. that non-U.S. companies can violate U.S. sanctions by *causing* – through initiating U.S. dollar payments – U.S.-based banks or branches to violate sanctions by engaging in the prohibited exportation of financial services from the United States for the benefit of sanctioned parties or jurisdictions.

On July 16, 2020, DOJ and OFAC announced parallel resolutions with Essentra FZE Company Limited (“Essentra”), a UAE-based supplier, for selling cigarette products it knew to be ultimately destined for North Korea.¹² The transactions involved documentation falsely naming China as the destination.

OFAC concluded that Essentra’s conduct of this business and its receipt of three payments into its bank accounts at the non-U.S. branch of a U.S. bank “caused” the branch (a U.S. person) to export, directly or indirectly, financial services to North Korea. Similarly, in DOJ and OFAC’s January 14, 2021, resolutions with PT Bukit Muria Jaya (“BMJ”), a paper products manufacturer located in Indonesia, BMJ “directed” payments for its North Korean exports to its USD bank account at a non-U.S. bank, which caused U.S. banks to clear wire transfers related to these exports.¹³ Non-U.S. companies are now on notice of the risk of *criminal* enforcement in addition to OFAC enforcement for the use of U.S. dollar transactions (or transactions denominated in other currencies utilising non-U.S. branches of U.S. banks) in connection with sanctioned-country business. To reduce their risks, non-U.S. companies should consider strengthening their sanctions compliance programmes, including training, controls, and employee oversight.

OFAC also recently issued its first and second public enforcement actions against cryptocurrency companies. First, on December 30, 2020, OFAC entered into a settlement with BitGo, Inc. (“BitGo”), a U.S. company that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services.¹⁴ OFAC determined that deficiencies in BitGo’s sanctions compliance procedures caused the company to fail to prevent persons it knew (based on IP address data) were located in sanctioned jurisdictions from using its non-custodial secure digital wallet management service. Similarly, on February 18, 2021, OFAC entered into a settlement with BitPay, Inc. (“BitPay”), a U.S. company that offers a payment processing solution for merchants to accept digital currency as payment, for processing payments on behalf of individuals who, based on IP addresses and information available in invoices, were located in sanctioned jurisdictions. Additionally, OFAC has recently focused on money service businesses (“MSBs”), as evidenced by its 2021 actions against Payoneer Inc. (“Payoneer”) and MoneyGram Payment Systems, Inc. (“MoneyGram”). OFAC stated that such digital currency businesses and MSBs, like other financial services providers, are responsible for ensuring compliance with OFAC sanctions, including understanding their sanctions-related risks and taking steps to mitigate against such risks.¹⁵

Utilising non-standard payment or commercial practices

The Framework notes that companies are best positioned to determine whether a particular dealing, transaction, or activity is performed in a manner consistent with industry practice. Sometimes deviations from standard practice are driven by an effort to evade or circumvent sanctions. For example, on January 4, 2021, OFAC entered into a \$8,572,500 settlement with Union de Banques Arabes et Françaises (“UBAF”), a French bank specialising in trade finance, for processing 127 payments on behalf of sanctioned Syrian financial institutions.¹⁶ The majority of the apparent violations involved UBAF’s processing of internal book-to-book transfers on behalf of Syrian entities that were followed by corresponding funds transfers through the U.S. financial system. The remaining violations were either “back-to-back” letter of credit transactions – where a sanctioned Syrian entity was the beneficiary of export letters of credit or the applicant for import letters of credit that did not involve USD clearing, but the intermediary entered into or received one or more corresponding USD letters of credit to purchase or sell the same goods – or other trade finance transactions involving sanctioned parties, all of which were processed through a U.S. bank. OFAC stated that UBAF’s actions during this time

period demonstrated knowledge of OFAC sanctions, but the bank incorrectly believed that avoiding direct USD clearing on behalf of sanctioned parties was sufficient for compliance. In other instances, a customer may ask for accommodation that results in a sanctions violation. In OFAC's May 2019 Haverly Systems Inc. ("Haverly") settlement, it was determined that the company collected a debt from an entity on the Sectoral Sanctions Identification ("SSI") List outside of the permitted maturity window.¹⁷ In this case, Haverly's Russian customer requested that Haverly reissue an invoice with a different date, in an attempt to re-characterise the debt as without the permitted maturity window.

Export or reexport of U.S.-origin goods

OFAC has regularly pursued enforcement actions against non-U.S. companies that purchased U.S.-origin goods with the intent of reexporting, transferring, or selling the items to a sanctioned person or jurisdiction. As noted in the Framework, some of OFAC's public enforcement actions in this area have focused on large or sophisticated entities that "engaged in a pattern or practice that lasted multiple years, ignored or failed to respond to numerous warning signs, utilised non-routine business practices, and – in several instances – concealed their activity in a wilful or reckless manner".¹⁸

For example, in April 2021, SAP SE ("SAP") entered into parallel resolutions with DOJ, OFAC, and BIS totalling around \$8 million regarding U.S. sanctions and export violations involving the export of software and related services to Iran.¹⁹ These resolutions involved, in part, SAP's release of U.S.-origin software to non-U.S. third parties who made the software available in Iran. OFAC determined that in some cases, SAP managers had direct knowledge and facilitated the purchase of this software. OFAC further determined that SAP had reason to know from IP address data that services were being downloaded in Iran. SAP was faulted for not adopting IP blocking technology to prevent such downloads. Additionally, several U.S.-based SAP subsidiaries allowed Iranian users to access U.S.-based cloud services. OFAC faulted SAP for allowing these subsidiaries to operate as standalone entities for years with respect to compliance, despite pre- and post-acquisition reports of significant compliance deficiencies.

Other OFAC actions in this area involve less egregious conduct. For example, in February 2020 OFAC reached a \$2.4 million settlement with the Swiss entity Société Internationale de Télécommunications Aéronautiques SCRL ("SITA") involving, in part, SITA's provision of U.S.-origin software for the benefit of sanctioned airlines and its provision of messaging services that routed through servers in the United States, where messaging went to or from sanctioned airlines or other parties that were providing services to those airlines.²⁰ The SITA action represents OFAC's first public enforcement action involving sets of violations where the only U.S. nexuses were the provision of U.S.-origin software by a non-U.S. person and the use of a U.S.-based server, respectively.

U.S. parent liability for non-U.S. subsidiary business; facilitating activities of non-U.S. affiliates

Multiple recent OFAC enforcement actions highlight OFAC's increased willingness to hold U.S. parent companies liable for the Iranian or Cuban business conducted by their non-U.S. subsidiaries. For example, in Berkshire Hathaway, Inc.'s ("Berkshire"), October 20, 2020 settlement, OFAC held Berkshire accountable

for its Turkish subsidiaries' sales to two Turkish intermediary companies with knowledge that these goods would be resold to Iran. OFAC found that these violations occurred despite the fact that Berkshire and other Berkshire subsidiaries repeatedly communicated with and sent policies to the Turkish subsidiary regarding Iran sanctions. The Turkish subsidiary nonetheless took steps to conceal its dealings with Iran, such as using private email addresses that bypassed the controls of the corporate email system, utilising false names and false invoices, and providing false responses to compliance inquiries. OFAC found that certain other Berkshire subsidiaries received information that could have revealed that orders might have been destined for Iranian end users – but only one Berkshire subsidiary flagged that transactions with Iranian customers were prohibited. These actions highlight the importance of performing appropriate due diligence in connection with the acquisition of non-U.S. entities and ensuring that subsidiaries of U.S. companies, and other entities controlled by U.S. companies, understand their obligations to comply with U.S. sanctions on Iran and Cuba, including when they supply goods to other companies within their corporate organisation.

Relatedly, multiple OFAC enforcement actions have involved U.S. firms referring business to, approving, or otherwise facilitating dealings with sanctioned persons or jurisdictions by their non-U.S. affiliates. On October 1, 2020, OFAC announced a \$5.8 million settlement with New York travel services company Generali Global Assistance, Inc. ("GGA") for apparent violations of Cuba sanctions. GGA intentionally referred Cuba-related payments to its Canadian affiliate to avoid processing reimbursement payments directly to Cuban parties and to travelers while they were located in Cuba. GGA subsequently reimbursed its Canadian affiliate for those payments.

Additionally, non-U.S. companies with U.S. operations should take steps to ensure that U.S. offices and employees are walled off or recused from any sanctioned business engaged in by non-U.S. parts of the company. In July 2021, OFAC penalised a U.S. subsidiary of Alfa Laval AB for its referral of an Iranian business opportunity to its non-U.S. affiliate.²¹ This case demonstrates the importance of adopting training to ensure U.S. persons know they are prohibited from referring or participating in business opportunities involving sanctioned jurisdictions.

Deficient due diligence

A fundamental element of sanctions compliance is conducting appropriate due diligence on customers, supply chains, intermediaries, and counterparties. OFAC has recently brought several enforcement actions resulting from deficient due diligence.

As demonstrated by OFAC's September 20, 2020 settlement with Deutsche Bank Trust Company Americas ("DBTCA"), financial institutions are expected to conduct appropriate diligence on transactions that raise sanctions red-flags prior to processing transactions.²² Specifically, OFAC faulted DBTCA for not independently corroborating verbal representations it received from the U.S. counsel of a non-account holder party to the transaction at issue in order to confirm that there was no SDN interest in the transaction. OFAC stated that although the payment transactions associated with the transaction did not contain an explicit reference to the SDN, the payment was "related to a series of purchases of fuel oil that involved" the SDN and that, at the time of the transaction, "DBTCA had reason to know of [the SDN's] potential interest in the transaction underlying the payment, which closely coincided [with the SDN's designation]". OFAC and other regulators expect companies to fully review all the documentation they receive for potential indicia of a nexus to a sanctioned jurisdiction or person prior to sending, approving, or facilitating a payment.

Similarly, OFAC expects that companies implement measures, beyond contractual provisions, to monitor and minimise sanctions risk over the life of a contractual relationship, such as a leasing agreement. In its settlement with U.S.-based Apollo Aviation Group LLC (“Apollo”), OFAC determined that Apollo leased three aircraft engines to a UAE company that subleased them to an airline in Ukraine that, in turn, installed the engines on an aircraft wet leased to an SDN.²³ When the engines were returned, Apollo discovered that the engines had been installed on aircraft owned by or leased to an SDN and used in Sudan (which, at the time, was subject to comprehensive U.S. sanctions). Although Apollo’s lease agreements with the UAE company included sanctions commitments, OFAC faulted Apollo Aviation for failing to take steps to monitor whether the engines were being used in a sanctions compliant manner.

Misinterpreting, or failing to understand the applicability of, OFAC’s regulations

Often companies will misunderstand the applicability or scope of OFAC’s sanctions prohibitions either because they are not aware of sanctions regulations or because they are unaware that such regulations apply to them by virtue of their status as U.S. persons, U.S.-owned subsidiaries (with respect to Cuba and Iran sanctions), or non-U.S. persons engaged in activities with a U.S.-nexus (involving U.S. persons, U.S.-origin goods, or U.S. territory, including payments transiting the U.S. financial system).

For example, on July 28, 2020, Whitford Worldwide Company, LLC’s (“Whitford”), settled with OFAC for conduct with Iran conducted by Whitford and its subsidiaries in Italy and Turkey.²⁴ Whitford’s Regulatory Affairs Manager had incorrectly advised that Whitford’s non-U.S. subsidiaries could continue selling to Iran legally as long as there were no direct connections between a subsidiary and Iran. As a result of this advice, Whitford developed a plan to continue selling to Iran, which required that all sales be directed through third-party distributors and that documents related to those sales avoid referencing Iran.

Another area of recent enforcement focus is the failure of companies to identify an applicable general licence or adhere to a general licence’s conditions, rendering the otherwise available authorisation inapplicable. For example, in OFAC’s May 2020 settlement with BIOMIN America, Inc., BIOMIN incorrectly believed that it could structure transactions involving a Cuban counterparty that would be consistent with OFAC’s Cuba sanctions.²⁵ BIOMIN coordinated and received commissions on sales to a Cuban counterparty as executed by BIOMIN’s non-U.S. affiliates. In determining that BIOMIN’s conduct resulted in violations, OFAC noted that the company could have availed itself of an existing general licence – if the exports had been licensed by the Commerce Department – or applied for a specific licence, and likely avoided the violations, but because the company appears not to have understood the scope of OFAC’s Cuba sanctions, it was not in a position to take advantage of these potential licensing avenues. Likewise, in OFAC’s July 2020 settlement with Amazon.com, Inc. (“Amazon”), OFAC determined that Amazon’s failure to abide by the reporting requirements associated with a general licence under its Ukraine-related sanctions effectively nullified that authorisation with respect to the affected transactions.

These actions demonstrate how companies can benefit from seeking appropriate advice and guidance when contemplating business involving U.S. sanctioned parties or jurisdictions. Management and sales teams would be wise to consult with internal and/or external legal or compliance experts to ensure that cross-border transaction structures do not run afoul of U.S. sanctions requirements. Such experts are also well positioned

to identify potential eligibility for authorisations from OFAC, including general and specific licences.

Screening software limitations; deficiencies in automated processes

Many companies screen their customers and other third parties, but such screening may be deficient due to a failure to adequately calibrate, update, or audit their screening software, lists, and procedures. A significant number of recent enforcement actions involved sanctions screening deficiencies, making it clear that the utilisation of defective screening software or insufficient screening lists will not provide a shield against regulatory enforcement.

For example, in its November 2018 settlement with Cobham Holdings, Inc. (“Cobham”), OFAC found that Cobham made three shipments of goods through distributors in Canada and Russia to an entity that did not appear on the SDN List, but which was blocked under OFAC’s “50 percent rule” because it was 51 per cent owned by a Russian SDN.²⁶ The apparent violations appear to have been caused by reliance on deficient third-party screening software. Although Cobham had selected “fuzzy” searching to detect partial matches, the software instead used an “all word” match criteria. The names of the blocked party and its subsidiary both contained several of the same uncommon words such that fuzzy searching apparently would have detected the match; however, under the “all word” criteria, the transactions were not flagged and were processed.

Additionally, in its settlement with Amazon, OFAC faulted, in part, the company’s failure to screen for a city within a sanctioned jurisdiction and common alternative spellings of a sanctioned jurisdiction. OFAC also determined that Amazon’s automated screening processes also failed to identify the correctly spelled names and addresses of persons on OFAC’s SDN List. And in a second September 2020 settlement with DBTCA, OFAC determined that DBTCA failed to stop payments destined for accounts at a designated financial institution because – contrary to its existing policies and procedures – DBTCA did not include in its sanctions screening tool the designated financial institution’s SWIFT Business Identifier Code.²⁷

OFAC’s April 30, 2020 finding of violation issued to American Express Travel Related Services Company (“Amex”), criticised Amex for approving an SDN’s customer application submitted by a non-U.S. bank due to system deficiencies.²⁸ When the non-U.S. bank entered the SDN’s information into the screening system, Amex’s “risk engine” identified the applicant as a potential SDN and generated multiple “declined” messages to the non-U.S. bank indicating that the application could not be processed. However, the non-U.S. bank made several additional approval attempts that caused the screening engine to time out, triggering the application to be automatically approved.

OFAC has stated that companies should carefully review and understand the functionality and limitations of their sanctions screening software, ensure sufficient staff training regarding the software, update the software accordingly, and periodically evaluate the software with test data to ensure that it sufficiently flags transactions even absent an exact match. Additionally, companies should ensure that automated sanctions compliance controls measures cannot be overridden without appropriate review. Companies should also ensure that the lists they screen against not only capture indicators for sanctioned jurisdictions – such as cities, regions, and ports within sanctioned jurisdictions – but also appropriate name variations for those locations. The Cobham settlement further suggests that, depending on their risk profile, companies should consider investing in systems for identifying entities that are treated as SDNs under OFAC’s 50 percent rule. In that settlement, OFAC recognised Cobham’s adoption of such a system as a risk-reducing measure.

Mergers and acquisitions

Multiple recent OFAC enforcement actions highlight the importance of performing adequate sanctions due diligence with regard to potential acquisition targets and to implementing strong sanctions compliance procedures following acquisition. Often, although these non-U.S. subsidiaries were required by their U.S. parents to cease their transactions with sanctioned jurisdictions, the non-U.S. subsidiaries failed to do so.

For example, in its September 24, 2020 settlement with OFAC Keysight Technologies, Inc. (“Keysight”), agreed to pay \$473,157 to settle violations of Iran sanctions on behalf of its former Finnish subsidiary, Anite Finland Oy (“Anite”).²⁹ Prior to Keysight’s acquisition of Anite in 2015, Anite had committed to cease all existing and future business with certain sanctioned countries, including Iran. After the acquisition, Keysight reiterated to Anite that sales to these countries must cease. Nevertheless, Anite’s Vice President for Europe, Middle East, and Africa and its Regional Director for the Middle East both expressed reluctance to comply. The Regional Director and two employees then took measures to obfuscate from Keysight their dealings with Iran, including omitting references to Iran in correspondence. Although Keysight conducted an internal investigation upon discovering the misconduct and voluntarily self-disclosed the violations, OFAC deemed Anite’s violations an egregious case due to the willful violations, active participation by senior managers, and attempts at concealment.

Individual liability

Historically, OFAC has generally not pursued enforcement actions against individuals outside of the Cuba-travel context. However, the Framework notes that “individual employees – particularly in supervisory, managerial, or executive-level positions – have played integral roles in causing or facilitating” sanctions violations, even in instances where “the U.S. entity had a fulsome sanctions compliance program in place” and in some cases these employees “made efforts to obfuscate and conceal their activities from others within the corporate organisation, including compliance personnel, as well as from regulators or law enforcement”.³⁰ The Framework states that, in such instances, OFAC will consider enforcement actions not only against the entities, but against the individuals as well.³¹

In 2019, OFAC took the unprecedented step of designating a former company manager as a foreign sanctions evader while concurrently announcing a settlement with the company’s U.S. parent.³² Specifically, OFAC designated the former managing director of the U.S. company’s Turkish subsidiary whom OFAC determined to be primarily responsible for directing the apparent violations at issue and seeking to conceal them. This designation highlights increased personal risk for personnel who play a central role in causing violations of U.S. sanctions law.

Conclusion

Although OFAC’s regulations do not themselves require the implementation of a compliance programme, OFAC’s Framework and the compliance guidance embedded in recent enforcement actions represent a new effort by OFAC to more clearly and comprehensively communicate its expectations about appropriate sanctions compliance practices. U.S. and non-U.S. companies alike would be well-advised to study this guidance and consider making appropriate enhancements to their compliance practices.

Endnotes

1. Paul, Weiss, *OFAC Issues Guidance on Sanctions Compliance Programs and Flags “Root Causes” Underlying Prior Enforcement Actions*, (May 14, 2019), available at <https://www.paul-weiss.com/practices/litigation/economic-sanctions-aml/publications/ofac-issues-guidance-on-sanctions-compliance-programs-and-flags-root-causes-underlying-prior-enforcement-actions?id=28725>.
2. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *A Framework for OFAC Compliance Commitments*, (May 2, 2019), available at <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.
3. OFAC considers “senior management” to “typically include senior leadership, executives, and/or the board of directors”. See Framework at 2.
4. *Id.* at 2–3.
5. *Id.* at 3.
6. *Id.* at 3–5.
7. *Id.* at 5–6.
8. *Id.* at 7.
9. See e.g., U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 19, 2018*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; *Enforcement Information for Apr. 15, 2019*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; see also Paul, Weiss, *UniCredit Group Banks Agree to Pay a Combined \$1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty* (May 1, 2019), available at <https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/unicredit-group-banks-agree-to-pay-a-combined-13-billion-penalty-for-iranian-and-other-sanctions-violations-one-bank-pleads-guilty?id=28671>.
10. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 19, 2018*, available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190415_uni_webpost.pdf; *Enforcement Information for Apr. 15, 2019*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; see also Paul, Weiss, *UniCredit Group Banks Agree to Pay a Combined \$1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty* (May 1, 2019), available at <https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/unicredit-group-banks-agree-to-pay-a-combined-13-billion-penalty-for-iranian-and-other-sanctions-violations-one-bank-pleads-guilty?id=28671>.
11. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 19, 2018*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; *Enforcement Information for Apr. 15, 2019*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; see also Paul, Weiss, *UniCredit Group Banks Agree to Pay a Combined \$1.3 Billion Penalty for Iranian and Other Sanctions Violations; One Bank Pleads Guilty* (May 1, 2019), available at <https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/unicredit-group-banks-agree-to-pay-a-combined-13-billion-penalty-for-iranian-and-other-sanctions-violations-one-bank-pleads-guilty?id=28671>.
12. See U.S. Dep’t of Justice, *Essentra Fze Admits to North Korean Sanctions and Fraud Violations, Agrees to Pay Fine* (July 16, 2020), available at <https://www.justice.gov/>

- opa/pr/essentra-fze-admits-north-korean-sanctions-and-fraud-violations-agrees-pay-fine (“DOJ Press Release”); Settlement Agreement between the U.S. Department of the Treasury’s Office of Foreign Assets Control and Essentra FZE Company Limited (July 16, 2020) available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information> (“OFAC Settlement Agreement”); see also Paul, Weiss, DOJ and OFAC Enforcement Actions Against Essentra FZE Signal New Sanctions Risks for Non-U.S. Companies Utilizing the U.S. Financial System (July 23, 2020), available at <https://www.paulweiss.com/media/3980400/23july20-doj-ofac.pdf>.
13. U.S. Dep’t of Justice, *Indonesian Company Admits To Deceiving U.S. Banks In Order To Trade With North Korea, Agrees To Pay A Fine Of More Than \$1.5 Million* (Jan. 17, 2021), available at <https://www.justice.gov/opa/pr/indonesian-company-admits-deceiving-us-banks-order-trade-north-korea-agrees-pay-fine-more-15>; U.S. Dep’t of Treasury, *OFAC Settles with PT Bukit Muria Jaya for Its Potential Civil Liability for Apparent Violations of the North Korea Sanctions Regulations* (Jan. 14, 2021), available at https://home.treasury.gov/system/files/126/20210114_BMJ.pdf.
 14. U.S. Dept. of Treasury, Office of Foreign Assets Control, *Enforcement Information for Dec. 30, 2020*, available at https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
 15. See U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 23, 2021*, available at https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf; U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for April 29, 2021*, available at https://home.treasury.gov/system/files/126/20210429_moneygram.pdf.
 16. U.S. Dep’t of Treasury, Office of Foreign Assets Control, *OFAC Enters Into \$8,572,500 Settlement with Union de Banques Arabes et Françaises for Apparent Violations of Syria-Related Sanctions Program* (Jan. 4, 2021), available at https://home.treasury.gov/system/files/126/01042021_UBAF.pdf.
 17. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Apr. 25, 2019*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>.
 18. Framework at 10.
 19. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Apr. 29, 2021*, available at https://home.treasury.gov/system/files/126/20210429_sap.pdf.
 20. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Feb. 26, 2020*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>. Paul, Weiss, *OFAC Cites the Use of U.S.-Origin Software and U.S. Network Infrastructure in Reaching a Nearly \$8 Million Settlement with a Swiss Commercial Aviation Services Company* (Mar. 16, 2020), available at <https://www.paulweiss.com/media/3979437/16mar20-ofac.pdf>.
 21. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 19, 2021*, available at https://home.treasury.gov/system/files/126/20210719_al.pdf.
 22. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Sept. 20, 2020*, available at https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
 23. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 7, 2019*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; see also Paul, Weiss, *OFAC Enforcement Action against U.S. Aviation Company Shows the Importance of Ongoing Monitoring over the Course of a Contractual Relationship* (Dec. 9, 2019), available at <https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/ofac-enforcement-action-against-us-aviation-company-shows-the-importance-of-ongoing-monitoring-over-the-course-of-a-contractual-relationship?id=30324>.
 24. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for July 28, 2020*, available at https://home.treasury.gov/system/files/126/20200728_whitford.pdf.
 25. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for May 2, 2019*, available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20200506_biomin.pdf.
 26. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Nov. 27, 2019*, available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181127_metelics.pdf; see also Paul, Weiss, *OFAC Reaches Settlement with Cobham Holdings, Inc. for Violations Resulting from Deficient Screening Software* (Nov. 29, 2018), available at <https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/ofac-reaches-settlement-with-cobham-holdings-inc-for-violations-resulting-from-deficient-screening-software?id=27872>.
 27. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Sept. 20, 2020*, available at https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
 28. U.S. Dep’t of Treasury, Office of Foreign Assets Control, *OFAC Issues a Finding of Violation to American Express Travel Related Services Company for Violations of the Weapons of Mass Destruction Proliferators Sanctions Regulations* (Apr. 30, 2020), available at https://home.treasury.gov/system/files/126/20200430_amex.pdf.
 29. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Sept. 24, 2020*, available at https://home.treasury.gov/system/files/126/20200924_keylight.pdf.
 30. Framework at 12.
 31. *Id.*
 32. U.S. Dep’t of the Treasury, Office of Foreign Assets Control, *Enforcement Information for Feb. 7, 2019*, available at <https://home.treasury.gov/policy-issues/financial-sanctions/civil-penalties-and-enforcement-information>; Paul, Weiss, *In Unprecedented Move, OFAC Takes Enforcement Action Against U.S. Parent Company for Turkish Subsidiary’s Iran Sanctions Violations and Simultaneously Sanctions the Subsidiary’s Ex-Managing Director* (Feb. 11, 2019), available at <https://www.paulweiss.com/media/3978456/11feb19-ofac-kollmorgen.pdf>.



Roberto J. Gonzalez is a litigation partner and the co-chair of the firm's Economic Sanctions and Anti-Money Laundering Practice Group. He represents global financial institutions, technology companies and other clients in civil and criminal investigations and enforcement matters relating to U.S. economic sanctions, export controls, and anti-money laundering. He also provides regulatory advice, compliance counselling, and transactional due diligence to U.S. and non-U.S. companies across a range of sectors. He writes and speaks frequently on these topics. Roberto joined Paul, Weiss after serving several years in senior legal positions at the U.S. Treasury Department, the Consumer Financial Protection Bureau, and the White House Counsel's Office. As Deputy General Counsel of the Treasury Department, Roberto supervised over a hundred lawyers – including the legal offices of OFAC and FinCEN – in the areas of sanctions, anti-money laundering, and financial regulation. He uses his multi-faceted experience in the federal government to help clients navigate the constantly evolving U.S. regulatory and enforcement landscape.

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, D.C., 20006-1047
USA

Tel: +1 202 223 7316
Email: rgonzalez@paulweiss.com
URL: www.paulweiss.com



Rachel M. Fiorill, Counsel in the Litigation Department, formerly served as an Enforcement Section Chief at the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").

At OFAC, Rachel led the investigation and resolution of hundreds of enforcement actions, including several groundbreaking civil monetary penalties. She served the Enforcement Division's lead for Ukraine/Russia and Syria-related investigations and developed particular expertise with OFAC's Iran sanctions while representing the Enforcement Division in agency-wide Joint Comprehensive Plan of Action ("JCPOA") implementation matters. She liaised with other law enforcement and intelligence agencies regarding joint investigations, enforcement priorities and strategies and provided guidance on OFAC's Economic Sanctions Enforcement Guidelines and sanctions programmes to counterparts at other agencies and the public.

She advises clients on government inquiries and investigations, sanctions compliance and risk management, and transactional due diligence. She counsels on a variety of financial crime and international trade issues, including economic sanctions, anti-money laundering, anti-corruption, and export controls.

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, D.C., 20006-1047
USA

Tel: +1 202 223 7346
Email: rfiorill@paulweiss.com
URL: www.paulweiss.com

Paul, Weiss is a firm of more than 1,000 lawyers with diverse backgrounds, personalities, ideas and interests who provide innovative and effective solutions. We take great pride in representing our clients in their most critical legal matters and most significant transactions, as well as individuals and organisations in need of *pro bono* assistance.

Our team advises U.S. and non-U.S. clients across industries on their most sensitive U.S. economic sanctions, export control, and Bank Secrecy Act/anti-money laundering (BSA/AML) issues. We provide regulatory advice and compliance counselling, apply for licences and interpretive guidance on behalf of clients, and perform transactional due diligence. With our preeminent regulatory defence and white collar experience, we are also uniquely positioned to: assist clients in responding to regulator inquiries, examinations, and subpoenas; conducting internal investigations; and handling matters that develop into multi-agency civil and criminal investigations.

www.paulweiss.com

Paul | Weiss

No End in Sight: An Update on the Rising Risk and Recent Developments in Cryptocurrency Sanctions and Enforcement

Guidehouse



Adam Klauder

I Introduction

Countries around the globe continue to use economic sanctions as a targeted means of implementing foreign policy objectives. By their nature, sanctions evolve continuously to address new threats and to advance a particular government's current foreign policy objectives. Due to its seamless peer-to-peer transfer capabilities, pseudo-anonymous qualities, and the still-maturing regulatory environment in which it exists, cryptocurrency has become an attractive alternative for criminals and other malign actors that seek to evade sanctions and move illicit funds across international borders.¹ Governments and regulators are responding to this rising risk through new guidance, regulation, and enforcement. Since the initial publication of this chapter in the 2020 edition of the *ICLG – Sanctions* guide, the pace of these developments has been swift and shows no sign of slowing down. This chapter will provide an updated overview of recent cryptocurrency developments for 2021, particularly as they relate to economic sanctions.

II Cryptocurrency Background

Cryptocurrencies are digital representations of value that, unlike government-issued fiat currency, do not have any status as legal tender. Some digital assets are “centralised”, meaning they have a central payment ledger that is run by a centralised administrator who issues currency. Cryptocurrencies, on the other hand, use “distributed” ledger technology (e.g., blockchain), to enable individual computers within peer-to-peer networks to record and share transactions in their respective electronic ledgers. Bitcoin, Ether, and Litecoin are some of the most well-known types of cryptocurrencies and are designed to function as a medium of exchange or payment for goods and services.²

Most cryptocurrencies use cryptographic protocols to both secure the ledger and make sure transactions that are recorded on the blockchain are public. Cryptocurrencies provide “pseudo-anonymity” to users because although a transaction can be associated with a specific cryptocurrency address, the name of the actual address holder is not visible on the blockchain and can remain anonymous.³ Law enforcement and the commercial sector have developed forensic and monitoring tools to help identify illicit actors who are associated with particular cryptocurrency addresses, but technology that allows individuals to process financial transactions with any level of anonymity can create a significant risk that sanctions evaders could seek to exploit.

Virtual currency exchanges provide platforms for customers to either trade cryptocurrencies for other cryptocurrencies, or to trade cryptocurrencies for fiat currency. Similar to banks, many virtual currency exchanges also store cryptocurrency for their customers. Most jurisdictions regulate cryptocurrency

exchanges as financial institutions, usually as money transmitters or payment services. Deemed to be money transmitters, virtual currency exchanges in the United States are required to comply with the Bank Secrecy Act (BSA) and its associated regulations, which involves conducting due diligence on customers and maintaining adequate anti-money laundering (AML) controls.⁴ In addition, the U.S., along with other countries and governmental bodies, have well-developed economic sanctions programmes that apply to cryptocurrency exchanges regardless of their regulatory status.

III U.S. Economic Sanctions and Cryptocurrency Developments

A. U.S. Economic Sanctions Overview

Economic sanctions are a tool that governments use to achieve foreign policy objectives by targeting specific individuals, entities, governments, and/or countries. In the United States, the Department of the Treasury's Office of Foreign Assets Control (OFAC) implements and administers economic sanctions under applicable U.S. laws.⁵ Generally, U.S. economic sanctions seek to deprive targets of the use of their assets and/or to deny them the benefits of trade and commerce with the United States.

All “U.S. persons” must comply with U.S. economic sanctions. This includes any U.S. citizen, permanent resident alien, entity organised under the laws of the United States, or any person in the United States. In the case of some OFAC sanctions, the prohibitions also apply to non-U.S. entities that are owned or controlled by U.S. persons.

U.S. economic sanctions can take the form of primary sanctions, which include list-based blocking sanctions that prohibit U.S. persons from undertaking almost all transactions related to the individuals and entities found on the list of Specially Designated Nationals and Blocked Persons (SDN). In addition, country-based embargoes prohibit U.S. persons from undertaking almost all transactions with a listed jurisdiction. Finally, list-based sectoral sanctions prohibit U.S. persons from undertaking limited, specific transactions with listed entities. Secondary sanctions seek to deter non-U.S. persons from engaging in a range of activities even if they do not involve any U.S. elements.

B. OFAC Cryptocurrency Developments

In March 2018, OFAC took an initial public step to address how it will treat compliance obligations relating to cryptocurrency by publishing five frequently asked questions (FAQs).⁶ These

FAQs confirm that a U.S. person's OFAC compliance obligations remain the same, regardless of whether a transaction is denominated in digital currency or in traditional fiat currency, and recommend that U.S. technology companies, payment processors, and digital currency administrators, exchangers, and users “develop a tailored, risk-based compliance program, which generally should include sanctions-list screening and other appropriate measures”⁷. OFAC further signalled that it might include digital currency addresses associated with blocked persons as identifiers on the SDN List.⁸ OFAC explained that parties who hold cryptocurrency and identify digital currency identifiers or wallets that they believe are owned by, or otherwise associated with, an SDN should take the necessary steps to block the relevant digital currency and file a report with OFAC that includes information about the wallet's or address's ownership, and any other relevant details.⁹ Importantly, OFAC clarified that “persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority”¹⁰. By publishing these FAQs, OFAC put the financial community on notice as to the level of compliance it expects from those who are engaged in cryptocurrency transactions.

In November 2018, OFAC added two additional FAQs, which addressed technical requirements relating to blocking digital currency.¹¹ Most notably, however, was OFAC's designation in the same action of two Iran-based individuals as SDNs for their involvement in financial transactions related to the “SamSam” ransomware scheme.¹² In the scheme, the illicit cyber actors required victims to pay a “ransom” in bitcoin to regain access to and control of their data. The two SDNs were digital currency exchangers who helped the cyber actors exchange the bitcoin into Iranian rial and deposit it into Iranian banks. In the SDN listing for these two individuals, OFAC for the first time listed digital currency addresses in the identifying information. OFAC highlighted the significance of this action in its press release, and stated that “[l]ike traditional identifiers, these digital currency addresses should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses”¹³. OFAC coordinated its designations with related law enforcement actions against two other Iranian criminal actors by the Department of Justice (DOJ) and the FBI.¹⁴

OFAC published digital currency addresses as identifiers again in August 2019 when it designated three individuals, one company, and the Zheng Drug Trafficking Organization (DTO) as significant foreign narcotics trafficker SDNs under the Foreign Narcotics Kingpin Designation Act.¹⁵ The press release referenced a related indictment that was also unsealed, which noted that the Zheng DTO “laundered its drug proceeds in part by using digital currency such as bitcoin, transmitted drug proceeds into and out of bank accounts in China and Hong Kong, and bypassed currency restrictions and reporting requirements”¹⁶. Almost a year later, OFAC designated four additional individuals as SDNs for providing support to the Zheng DTO, and one company for being owned or controlled by the Zheng DTO.¹⁷

In October 2020, OFAC and the Financial Crimes Enforcement Network (FinCEN) issued concurrent advisories on the sanctions and AML risks relating to ransomware and the facilitation of ransomware payments (FinCEN's advisory will be discussed in Section IV.A. below). OFAC's advisory addresses the increase in ransomware payments demands over the past few years and the risks of making such payments, including that they will be made to parties with a sanctioned nexus and/or used to harm the national security interests of the United States.¹⁸ OFAC states clearly that any ransomware payments made to sanctioned parties result in penalties that are subject to strict liability and that any licence applications

involving ransomware payments will be reviewed by OFAC on a case-by-case basis with a presumption of denial. OFAC's advisory does, however, outline the steps that companies should take if they are victims of a ransomware attack, and notes that it would “consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus”¹⁹.

OFAC has continued to add digital currency addresses to the SDN List, including in April 2021, when it published a list of cryptocurrency addresses tied to alleged Russian governmental interference in U.S. elections.²⁰ These addresses were associated with a wide range of digital assets, including Bitcoin, Bitcoin Cash, Litecoin, Zcash, Dash, Verge and Ether.

In May 2021, OFAC updated FAQ 594, which had stated previously that it was not possible to search for digital currency addresses against OFAC's Sanctions List Search tool. The updated FAQ now reflects that such searches are possible, though only exact matches will be recognised (i.e., there is no “fuzzy logic”).²¹

C. State-sponsored Virtual Currencies

Many countries, including the United States, United Kingdom, and China, have explored creating state-sponsored or central bank cryptocurrencies. These efforts, which could create a means of transferring currency outside the traditional banking system, could pose a significant challenge to countering the sanctions evasion ambitions of countries such as Iran, North Korea, Russia and Venezuela.

1. Iran

In July 2018, Iran announced that it intended to launch a national cryptocurrency, which would be pegged to the rial, its national fiat currency.²² News reports indicated that the Iranian government has subsequently sought to ban any unapproved cryptocurrencies for payment purposes, but that it would permit individuals to hold small amounts of non-governmental cryptocurrencies for personal (i.e., non-commercial) purposes.²³ Regardless of the obvious tension that exists in Iran between the regime's development of a centralised national cryptocurrency and the desire of Iranian citizens to utilise decentralised cryptocurrencies, Iranians in both the government and the private sector will likely continue to look for ways to use this new type of asset to mitigate the ongoing economic effects of international sanctions.

2. Venezuela

In December 2017, Venezuela announced its plans to launch a state-sponsored cryptocurrency backed by oil reserves and commodities (the petro).²⁴ In response, President Trump issued Executive Order 13827²⁵ and OFAC issued additional FAQs that prohibit U.S. persons from engaging in transactions involving petros.²⁶ In March 2019, OFAC also designated Evrofinance Mosnarbank, a Moscow-based bank that is jointly owned by Russian and Venezuelan state-owned companies, as an SDN. OFAC described the bank as “the primary international financial institution willing to finance the petro”²⁷.

Although the petro has struggled to gain widespread traction as a viable currency alternative, Venezuela has developed a growing peer-to-peer market for cryptocurrency to protect against rising inflation.²⁸ In a recent action that could further impact Venezuela's petro ambitions, the United States has placed Joselit de la Trinidad Ramirez Camacho, the superintendent of Venezuela's petro initiative, on its “Most Wanted List” due to his alleged involvement in narcotics trafficking.²⁹

In August 2021, Venezuela announced that it would launch the country's first central bank digital currency, which will coincide

with a “monetary redenomination” to address high levels of inflation.³⁰ The Central Bank of Venezuela is expected to begin circulating the new digital Venezuelan bolivar in October 2021.

3. North Korea

News reports indicate that North Korea is also developing its own official cryptocurrency in a likely attempt to circumvent sanctions, though it appears to only be in the early stages of creation at the moment.³¹ With respect to cryptocurrency, North Korea is more well known for its state-sponsored cyber campaigns to hack cryptocurrency exchanges and launch ransomware attacks, as well as its cryptocurrency mining efforts. For example, the North Korean-linked Lazarus Group has been implicated in the 2017 WannaCry ransomware attack, which affected hundreds of thousands of computers worldwide, including the United Kingdom’s National Health Service.³² In September 2018, the United States filed charges against Lazarus Group member Park Jin Hyok for his involvement in this ransomware attack, along with his involvement in “the 2016 theft of \$81 million from Bangladesh Bank; the 2014 attack on Sony Pictures Entertainment; and numerous other attacks or intrusions on the entertainment, financial services, defense, technology, and virtual currency industries, academia, and electric utilities”.³³ In 2021, the DOJ unsealed an indictment against Park Jin Hyok and two other North Korean computer programmers for these wide-ranging offences.³⁴ The indictment also detailed a scheme to develop and market a digital token (the “Marine Chain Token”), which would allow investors to purchase fractional ownership interests in marine shipping vessels. According to the indictment, the purpose of this scheme was to evade U.S. sanctions, and the involvement of North Korean individuals was not disclosed during the perpetrators’ attempts to obtain funds from investors.

4. Russia

Although Russia has shown some resistance to fully embracing the use of cryptocurrencies, it has begun exploring the development of a state-sponsored cryptocurrency, with Russian officials stating that the primary goal is to “settle accounts with our counterparties all over the world with no regard for sanctions”.³⁵ In addition, news reports indicate that the Russian government was instrumental in helping Venezuela develop its state-sponsored petro cryptocurrency.³⁶ There had been a fear within Russia that all cryptocurrency activity would be banned as Russia and its central bank continue to work through how to maintain control over the cryptocurrency market without allowing its prevalence to erode the domestic markets and currency. Recently, however, Russia enacted a new cryptocurrency law that, beginning in 2021, will permit Russians to mine, own, and trade cryptocurrencies on exchanges as long as the cryptocurrency is not used for domestic goods and services.³⁷ Similar to Venezuela, Russia is making progress on developing a central bank digital currency, with a prototype slated to be ready by the end of 2021.³⁸

IV Sanctions and Regulatory Landscape

In addition to OFAC, other U.S. and global agencies such as FinCEN, the Financial Action Task Force (FATF), the DOJ, and the UN have been involved in developing guidance to raise awareness around the use of cryptocurrency for illicit purposes.

A. FinCEN

FinCEN implements, administers, and enforces compliance with the BSA and its associated regulations. In March 2013, FinCEN clarified that administrators and exchangers of virtual currency

are considered money services business (MSB) money transmitters and must register as such with FinCEN, as well as implement relevant AML recordkeeping, reporting, and compliance measures.³⁹ Since that time, FinCEN has been active in issuing guidance relating to cryptocurrencies and in helping financial institutions identify and address cryptocurrency compliance issues.

In October 2018, FinCEN issued an advisory on the Iranian regime’s attempts to exploit the international financial system.⁴⁰ This advisory sought to help U.S. financial institutions (including virtual currency administrators and exchangers) better detect potentially illicit transactions involving Iran. The advisory cautioned that although cryptocurrency is not used widely in Iran, it is “an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions”. As such, FinCEN urged financial institutions to consider reviewing blockchain ledgers for activity that may originate or terminate in Iran and advised them to be aware of person-to-person exchangers (i.e., natural or legal persons who offer to buy, sell, or exchange virtual currency through online sites and in-person meetups) that may offer services in Iran. The advisory reminded financial institutions that a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/Combating the Financing of Terrorism (CFT) obligations, as well as OFAC jurisdiction.

In May 2019, FinCEN issued an additional advisory on illicit activity such as money laundering and sanctions evasion involving “convertible virtual currencies” (CVCs).⁴¹ Specifically, the advisory highlights prominent typologies such as darknet marketplaces, peer-to-peer exchangers, foreign-located MSBs, and CVC kiosks, along with associated red flags. FinCEN issued concurrent guidance on how its regulations apply to certain businesses that transact in CVCs, which consolidated FinCEN’s previously issued guidance on this subject.⁴² FinCEN reiterated its general position that any person engaging in the business of money transmission or the transfer of funds, including CVCs, must (1) maintain an effective written AML programme, and (2) register as an MSB. FinCEN also required money transmitters that engage in a “transmittal of funds” to comply with the “Funds Transfer Rule”⁴³ and “Funds Travel Rule”.⁴⁴

During a speech in December 2019, FinCEN Director Ken Blanco noted that shortly after FinCEN issued its May advisory on illicit activity involving CVCs there were over 2,100 unique suspicious activity report (SAR) filers that referenced the key terms from the advisory, many of whom had not filed SARs previously.⁴⁵ With respect to cryptocurrencies, Director Blanco stated, “I think it is important for all financial institutions to ask themselves whether they are reporting such suspicious activity. If the answer is no, they need to reevaluate whether their institutions are exposed to cryptocurrency”.⁴⁶

As mentioned previously, FinCEN and OFAC released advisories in October 2020 to address the financial crime risks associated with ransomware and facilitating ransomware payments. The FinCEN advisory focuses on the role of financial intermediaries in the processing of ransomware payments, and outlines some of the current trends and typologies of ransomware and associated payments.⁴⁷ Some trends and typologies include cybercriminals targeting of larger enterprises to demand bigger payouts (i.e., “big game hunting”) and the use of anonymity-enhanced cryptocurrencies in illegal activity. The FinCEN advisory also lists 10 financial red flag indicators of ransomware-related illicit activity and reminds financial institutions of their reporting and information-sharing obligations related to ransomware attacks. In particular, FinCEN directs financial institutions to reference “CYBER-FIN-2020-A006” and include a narrative description in their SARs when there is a connection between the suspicious activity being reported and ransomware-related activity.

B. FATF

On June 21, 2019, FATF released new guidance governing virtual assets and virtual asset service providers.⁴⁸ The new FATF standards require all countries to regulate and supervise such service providers, including exchangers, and to mitigate against such risks when engaging in cryptocurrency transactions. This guidance represents a significant step toward strengthening international compliance standards around cryptocurrencies and recommends that the sector comply with the same AML/CFT requirements as traditional financial institutions. In June 2020, FATF issued a report that summarised its 12-month review of the industry's progress in implementing the new standards.⁴⁹ The report noted that 35 out of 54 reporting jurisdictions have implemented the revised FATF Standards and did not identify a clear need to amend the standards. It also acknowledged the progress that countries have made in implementing the "travel rule", which requires virtual asset service providers to obtain, hold and exchange information about the originators and beneficiaries of virtual asset transfers.⁵⁰ FATF issued its second 12-month review report in July 2021, which noted that even though an increased number of countries have implemented the revised FATF Standards and taken enforcement action against rule violators, most jurisdictions still have not implemented comprehensive AML/CFT requirements for virtual assets.⁵¹ In addition, the report noted that most jurisdictions are still not in compliance with the travel rule.

C. DOJ

On October 8, 2020, the DOJ Office of the Deputy Attorney General's Cyber-Digital Task Force, published "Cryptocurrency: An Enforcement Framework" (the Framework), which highlights the emerging criminal and national security threat that cryptocurrency use poses to the U.S. and provides detailed information about the DOJ's approach to combatting the illicit uses of cryptocurrency and related technologies.⁵² The Framework begins with an overview of cryptocurrency and some of its key characteristics (e.g., decentralised in nature, varying degrees of anonymity), and then describes in some detail both the legitimate and illegitimate uses of this type of virtual asset. In focusing on the ways in which malicious actors leverage cryptocurrency for criminal and illegal purposes, the Framework identifies various ways in which cryptocurrency can be used for illicit activity, including to commit crimes, support terrorism, or to hide financial activity. The Framework provides examples of recent enforcement actions that highlight various criminal schemes involving cryptocurrency, such as cases relating to ransomware, darknet markets, terrorist financing, money laundering, and operating unlicensed money services businesses. It also presents the current cryptocurrency regulatory landscape, including applicable laws and regulations, as well as relevant regulatory authorities. In its final section, the Framework identifies the types of business models and activities that may facilitate cryptocurrency-related criminal activity, as well as strategies that DOJ expects to deploy in response.

D. United Nations

The UN has published two recent annual reports that detail the extent to which North Korea has violated international sanctions, from procuring weapons of mass destruction to evading sanctions through maritime transactions. These reports also

detail some of the disruptive strategies that North Korea has been using to increase its financial position through both the theft and use of cryptocurrencies.

The August 2019 UN Panel of Experts Report listed 35 potential instances in which persons and/or entities affiliated with North Korea have attempted to generate revenue by engaging in cyber-related attacks on financial institutions, and stealing/mining cryptocurrency.⁵³ The report notes that a large number of targets in South Korea have come under attack by North Korea-affiliated entities, including the Bithub and Youbit cryptocurrency exchanges. In addition, the report describes how North Korea-affiliated actors have used cryptocurrency to launder bitcoin that was paid by victims of the WannaCry ransomware attacks.

The United Nations published a follow-up report in March 2020, where it highlighted additional ways in which North Korea has sought to generate illicit cryptocurrency revenue in contravention of international sanctions.⁵⁴ One unique way was by hosting a cryptocurrency conference in Pyongyang, which sought to involve experts from around the world. Virgil Griffith, a U.S. person who attended the 2019 conference, has been charged with violating U.S. sanctions. According to the pleadings, conference organisers instructed Griffith to explain how to use cryptocurrency and blockchain technology to evade sanctions and launder money.⁵⁵ In advance of the proposed February 2020 conference in North Korea there were press reports about the UN's warnings that attendance could constitute sanctions evasion.⁵⁶

The March 2020 UN Panel of Experts Report also details an additional cyber-attack by North Korea-affiliated actors against a cryptocurrency exchange that utilised a "Trojan horse" malware application, which allowed the hackers to control their victims' computer systems and access and steal cryptocurrency.⁵⁷

V Recent Enforcement Actions

March 2020 – DOJ Criminal Action Against Two Chinese Nationals for Laundering Over \$100 Million in Cryptocurrency from Exchange Hack

On March 2, 2020, the U.S. Department of Justice charged Chinese nationals Jiadong Li and Yinyin Tian with laundering over \$100 million worth of cryptocurrency from a hack of a cryptocurrency exchange.⁵⁸ In a coordinated action, OFAC designated Li and Tian as SDNs and added 20 new bitcoin addresses associated with these two individuals to the SDN List.⁵⁹ The civil forfeiture complaint specifically names 113 virtual currency accounts and addresses that were used by the defendants and unnamed co-conspirators to launder funds.

According to the pleadings, Li and Tian stole approximately \$250 million in cryptocurrency by hacking into a virtual currency exchange. To launder the funds, Li and Tian circumvented the compliance controls at various virtual currency exchanges by submitting falsified "know your customer" information and used "peel chains" to launder the stolen cryptocurrency and obscure the source of funds. In a peel chain, criminals "peel" off a small amount of cryptocurrency from a larger amount during a transaction. The process is repeated until all of the cryptocurrency has been sent to new addresses and it is often deposited into various virtual currency exchanges. Li and Tian spent several months using peel chains to transfer and convert much of the stolen cryptocurrency into regular currency at Chinese banks. The pleadings also indicate that Li and Tian sold some of the stolen cryptocurrency to U.S. customers and routed some of the funds through a U.S.-based cryptocurrency exchange.

On August 27, 2020, DOJ filed a civil forfeiture complaint to seize 280 cryptocurrency accounts containing funds that were laundered by the same group of Chinese actors.⁶⁰ This action also represents the first publicly announced case where North Korean hackers have targeted a U.S. virtual currency exchange.⁶¹

August 2020 – DOJ’s “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns”

On August 13, 2020, DOJ announced that it had dismantled three cyber-related terrorist financing campaigns involving the al-Qassam Brigades (Hamas’s military wing), al-Qaeda, and Islamic State of Iraq and the Levant (ISIS).⁶² DOJ noted that this coordinated operation was the U.S. government’s largest-ever seizure of cryptocurrency in the terrorism context, involving millions of dollars and over 300 cryptocurrency accounts.

According to the pleadings, the al-Qassam Brigades, which along with Hamas is designated by OFAC as an SDN, sought to solicit bitcoin donations to fund terrorism. U.S. law enforcement worked covertly to monitor and operate al-Qassam Brigade websites, which led to the seizure of approximately 150 cryptocurrency accounts that contained these illicit donations. The al-Qaeda campaign also involved solicitation for bitcoin donations to fund terrorism and used layering techniques to launder and obscure the source of the funds. U.S. law enforcement is seeking the forfeiture of the 155 virtual currency assets tied to this terrorist campaign. Finally, in the separate ISIS campaign, an ISIS hacker set up a website (FaceMaskCenter.com) and four Facebook pages to sell N95 respirator masks that had not been approved by the U.S. Food and Drug Administration. DOJ officials noted separately that the complaints did not identify any financial crime control failures at the institutions and regulated exchanges that handled the illicit cryptocurrency at issue.⁶³

December 2020 – OFAC Enters Into \$98,830 Settlement with BitGo, Inc., for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions

On December 30, 2020, OFAC announced its first enforcement action against a digital assets company. In the enforcement release, OFAC alleged that between approximately March 2015 and December 2019, California-based BitGo, Inc. (BitGo) had processed 183 digital currency transactions on behalf of individuals located in Crimea, Cuba, Iran, Sudan, and Syria, using BitGo’s “hot wallet” secure digital management service. According to OFAC, BitGo collected and tracked its users’ Internet Protocol (IP) addresses for security purposes related to account logins but did not use this same IP address information to identify and mitigate sanctions compliance risk. OFAC also noted that although BitGo amended its practices to require all new account holders to verify the country in which they were located beginning in April 2018, the company relied on user attestations and did not conduct additional verification or diligence on the location of its account holders.

This enforcement action is significant not only because it is the first one brought publicly by OFAC, but also because of the examples OFAC provides for good compliance practices for digital assets companies in the “mitigating factors” section of the enforcement release. OFAC notes that BitGo had invested in significant remedial measures, including hiring a chief compliance officer and implementing a new OFAC policy. With respect to BitGo’s policy, OFAC highlighted the following items, including:

- A detailed overview of OFAC and relevant sanctions laws.
- The appointment of a compliance officer specifically responsible for implementing and providing guidance and interpretation on matters related to U.S. sanctions laws.
- IP address blocking, as well as email-related restrictions, for sanctioned jurisdictions.
- Periodic batch screening.
- Record-keeping procedures for all financial records and documentation related to sanctions compliance efforts.
- A review and, where appropriate, update of end-user agreements to ensure that customers are aware of, and comply with, U.S. sanctions requirements.
- A review of screening configuration criteria on a periodic basis.

Even though OFAC determined that BitGo did not voluntarily disclose the matter and could have been subject to a maximum civil monetary penalty of approximately \$53 million, it determined that the case was “non-egregious” and entered into a settlement for \$98,830.

February 2021 – OFAC Enters Into \$507,375 Settlement with BitPay, Inc., for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions

Shortly after the BitGo enforcement action was released, OFAC announced its second enforcement action against a digital assets company. On February 18, 2021, OFAC issued an enforcement release in which it is alleged that BitPay, Inc. (BitPay) had processed 2,102 transactions between approximately June 2013 and September 2018 on behalf of individuals who were located in Crimea, Cuba, North Korea, Iran, Sudan, and Syria. BitPay is an Atlanta-based company that provides a payment processing solution for merchants to accept payment for goods in digital currency. OFAC alleged that although BitGo conducted sanctions screening on the merchants, who were BitGo’s direct customers, it did not screen the information it had in its possession relating to the merchants’ buyers, including their names, addresses, email addresses, and phone numbers.

Even though OFAC determined that BitPay did not voluntarily disclose the matter and could have been subject to a maximum civil monetary penalty of approximately \$620 million, it determined that the case was “non-egregious” and entered into a settlement for \$507,375.

VI Looking Toward the Future

There have been a number of important “firsts” and enforcement developments in the past year that highlight sanctions compliance issues and address potential sanctions evasion concerns, from OFAC bringing its first enforcement action against a digital assets company to the recent guilty plea from the former chief of darknet-based cryptocurrency “mixing” service Helix to money laundering conspiracy charges.⁶⁴ Even with increased guidance and law enforcement focus, however, illicit actors will likely continue attempting to exploit gaps in the regulatory framework and the ease of peer-to-peer transfer to use cryptocurrency to avoid economic sanctions. As a result, those who have cryptocurrency compliance obligations should review their compliance programmes to ensure that they are comprehensive and take current developments into account.

Consistent with OFAC’s compliance guidance, firms should conduct a risk assessment to identify potential OFAC issues that might exist as the result of their involvement with cryptocurrencies. In addition, institutions should update their screening

capabilities to incorporate the latest blockchain analytics solutions or engage with a vendor that can provide these services. Finally, firms should provide training to employees on blockchain technology, sanctions evasion typologies that are unique to cryptocurrencies, and recent developments in the cryptocurrency regulatory and enforcement area.

Endnotes

1. This chapter uses the term “cryptocurrency” to refer generally to “digital currency”, “virtual currency”, “virtual assets” and other similar terms to describe digital representations of value that can be traded digitally and function like money.
2. Rebecca M. Nelson, “Examining Regulatory Frameworks for Digital Currencies and Blockchain”, Testimony before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, July 30, 2019, <https://crsreports.congress.gov/product/pdf/TE/TE10034>.
3. Toshiendra Kumar Sharma, “How is Blockchain Verifiable by Public and Yet Anonymous?”, Blockchain Council, July 10, 2018, <https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/>.
4. 31 U.S.C. § 5311 *et seq.*
5. In addition to OFAC, other U.S. governmental agencies help enforce sanctions, including: (i) Department of State; (ii) Department of Justice; and (iii) the Department of Commerce, Bureau of Industry and Security (BIS). Many non-U.S. countries and governmental organisations also administer sanctions internationally, including: (i) the United Nations (UN); (ii) the European Union (EU); and (iii) the United Kingdom (Office of Financial Sanctions Implementation).
6. OFAC FAQs, Questions on Virtual Currency, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>.
7. *Id.*
8. OFAC FAQ 561, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>.
9. OFAC FAQ 562, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>.
10. OFAC FAQ 560, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>.
11. OFAC FAQs 646 and 647, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546>.
12. OFAC, “Cyber-related Designations; Publication of New Cyber-related FAQs”, November 18, 2018, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20181128>.
13. U.S. Department of the Treasury, Press Release: “Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses”, November 28, 2018, <https://home.treasury.gov/news/press-releases/sm556>.
14. U.S. Department of Justice, Press Release: “Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over \$30 Million in Losses”, November 28, 2018, <https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public>.
15. OFAC, “Kinpun Act Designations”, August 21, 2019, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20190821>.
16. U.S. Department of the Treasury, Press Release: “Treasury Targets Chinese Drug Kingpins Fueling America’s Deadly Opioid Crisis”, August 21, 2019, <https://home.treasury.gov/news/press-releases/sm756>.
17. U.S. Department of the Treasury, Press Release: “Treasury Targets Chinese Persons Involved with Drug Trafficking Organization Moving Fentanyl”, July 17, 2020, <https://home.treasury.gov/news/press-releases/sm1063>; OFAC, “Counter Narcotics Designations; Counter Narcotics Designations Removals and Update; Nicaragua-related Designations”, July 17, 2020, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200717>.
18. OFAC, “Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,” October 1, 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.
19. *Id.*
20. OFAC, “Issuance of Executive Order Blocking Property With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation and related Frequently Asked Questions; Russia-related Designations”, April 15, 2021, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210415>.
21. OFAC FAQ 594, <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626>.
22. Tanvi Ratna, “Iran Has a Bitcoin Strategy to Beat Trump”, Foreign Policy, January 24, 2020, <https://foreignpolicy.com/2020/01/24/iran-bitcoin-strategy-cryptocurrency-blockchain-sanctions/>.
23. Leigh Cuen, Stan Higgins, “Iran Could Ban Bitcoin for Payments, Central Bank Report Suggests”, *coindesk*, January 29, 2019, <https://www.coindesk.com/iran-could-ban-bitcoin-for-payments-central-bank-report-suggests>.
24. “Venezuela Plans a Cryptocurrency, Maduro Says”, *The New York Times*, December 3, 2017, <https://www.nytimes.com/2017/12/03/world/americas/venezuela-cryptocurrency-maduro.html>.
25. Executive Order 13827, “Taking Additional Steps to Address the Situation in Venezuela”, 83 Fed. Reg. 55, March 21, 2018, <https://home.treasury.gov/system/files/126/13827.pdf>.
26. OFAC, “Issuance of Venezuela-related Executive Order; Venezuela-related Designations; Publication of new Venezuela-related Frequently Asked Questions; Publication of new Digital Currency-related Frequently Asked Questions”, March 19, 2018, <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20180319>.
27. U.S. Department of the Treasury, Press Release, “Treasury Sanctions Russia-based Bank Attempting to Circumvent U.S. Sanctions on Venezuela”, March 11, 2019, <https://home.treasury.gov/news/press-releases/sm622>.
28. Caitlin Reilly, “Venezuelans use cryptocurrency to bypass corruption, inflation”, *Roll Call*, September 10, 2019, <https://www.rollcall.com/2019/09/10/venezuelans-use-cryptocurrency-to-bypass-corruption-inflation/>.
29. Paddy Baker, “US Offers \$5M Bounty for Arrest of Venezuela’s Crypto Chief”, *coindesk*, June 2, 2020, <https://www.coindesk.com/us-venezuela-petro-most-wanted>.
30. *Cointelegraph*, “Venezuela to launch CBDC in October – And cut six zeros from its currency”, August 6, 2021, <https://cointelegraph.com/news/venezuela-to-launch-cbdc-in-october-and-cut-six-zeros-from-its-currency>.
31. David Gilbert, “North Korea Is Building Its Own Bitcoin”, *Vice News*, September 18, 2019, https://www.vice.com/en_us/article/9ke3ae/north-korea-is-building-its-own-bitcoin.

32. Chris Graham, “NHS Cyber Attack: Everything You Need to Know About the ‘Biggest Ransomware’ Offensive in History”, *The Telegraph*, May 20, 2017, <https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>.
33. U.S. Department of Justice, “North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions”, September 6, 2018, <https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and>.
34. U.S. Department of Justice, “Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe,” February 17, 2021, <https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and>.
35. Max Seddon and Martin Arnold, “Putin considers ‘cryptorouble’ as Moscow seeks to evade sanctions”, *Financial Times*, January 1, 2018, <https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da>.
36. Simon Shuster, “Exclusive: Russia Secretly Helped Venezuela Launch a Cryptocurrency to Evade U.S. Sanctions”, *TIME*, March 20, 2018, <https://time.com/5206835/exclusive-russia-petro-venezuela-cryptocurrency/>.
37. Roger Huang, “Russia Backs Away From Total Cryptocurrency Ban”, *Forbes*, August 10, 2020, <https://www.forbes.com/sites/rogerhuang/2020/08/10/russia-backs-away-from-total-cryptocurrency-ban/#2a095c707520>.
38. CNBC, “Digital currencies are the future for Russia’s financial system, central bank governor says,” June 2, 2021, <https://www.cnbc.com/2021/06/02/digital-currencies-are-the-future-for-russia-central-bank-chief-says.html>.
39. FinCEN Guidance, FIN-2013-G001, “Application of FinCEN’s Regulations to Person’s Administering, Exchanging, or Using Virtual Currencies”, March 18, 2013, <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.
40. FinCEN Advisory, FIN-2018-A006, “Advisory on the Iranian Regime’s Illicit and Malign Activities and Attempts to Exploit the Financial System”, October 11, 2018, <https://fas.org/irp/world/iran/fincen-102018.pdf>.
41. FinCEN Advisory, FIN-2019-A003, “Advisory on Illicit Activity Involving Convertible Virtual Currency”, May 9, 2019, <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.
42. FinCEN Guidance, FIN-2019-G001, “Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies”, May 9, 2019, <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.
43. 31 CFR § 1010.410(e).
44. 31 CFR § 1010.410(f).
45. Ken Blanco, American Bankers Association/American Bar Association, Financial Crimes Enforcement Conference, December 10, 2019, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-american-bankers>.
46. *Id.*
47. FinCEN Advisory, FIN-2020-A006, “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments”, October 1, 2020, <https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf>.
48. FATF, “Guidance for a Risk-Based Approach, Virtual Assets and Virtual Service Providers”, June 21, 2019, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.
49. FATF, “12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers”, June 2020, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPs.pdf>.
50. Although progress has been made in this area, compliance will remain difficult to achieve until a workable technology solution is developed.
51. FATF, “Second 12-month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers”, July 2021, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPs.pdf>.
52. DOJ, “Report of the Attorney General’s Cyberdigital Task Force: Cryptocurrency Enforcement Framework”, October 2020, <https://www.justice.gov/archives/ag/page/file/1326061/download>.
53. United Nations, “Report of the Panel of Experts established pursuant to resolution 1874 (2009)”, August 30, 2019, <http://undocs.org/S/2019/691>.
54. United Nations, “Report of the Panel of Experts established pursuant to resolution 1874 (2009)”, March 2, 2020, <https://undocs.org/S/2020/151>.
55. Southern District of New York, *United States of America v. Virgil Griffith*, Case No. 19MAG10987, Complaint, November 21, 2019, <https://www.justice.gov/usao-sdny/press-release/file/1222646/download>.
56. Michele Nichols, “Exclusive: U.N. sanctions experts warn — stay away from North Korea cryptocurrency conference”, *Reuters*, January 15, 2020, <https://www.reuters.com/article/us-northkorea-sanctions-un-exclusive/exclusive-u-n-sanctions-experts-warn-stay-away-from-north-korea-cryptocurrency-conference-idUSKBN1ZE015>.
57. United Nations, “Report of the Panel of Experts established pursuant to resolution 1874 (2009)”, March 2, 2020, <https://undocs.org/S/2020/151>.
58. U.S. Department of Justice Press Release, “Two Chinese Nationals Charged with Laundering Over \$100 Million in Cryptocurrency from Exchange Hack”, March 2, 2020, <https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack>.
59. U.S. Department of the Treasury Press Release, “Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group”, March 2, 2020, <https://home.treasury.gov/news/press-releases/sm924>.
60. U.S. Department of Justice Press Release, “United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors”, August 27, 2020, <https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges>.
61. Ian Talley, “U.S. Moves to Seize Cryptocurrency Accounts Linked to North Korean Heists”, *Wall Street Journal*, August 27, 2020, <https://www.wsj.com/articles/u-s-moves-to-seize-cryptocurrency-accounts-linked-to-north-korean-heists-11598564571>.
62. U.S. Department of Justice Press Release, “Global Disruption of Three Terror Finance Cyber-Enabled Campaigns”, August 13, 2020, <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>.

63. Valentina Pasquali, “US Prosecutors Announce ‘Historic’ Takedown of Global ‘Terrorists’ Crypto Networks”, ACAMS moneylaundering.com, August 13, 2020, https://www.moneylaundering.com/news/us-prosecutors-announce-historic-takedown-of-global-terrorists-crypto-networks/?source=Keyword%20Alert%20-%20Daily&utm_campaign=&utm_medium=email&utm_source=Eloqua&utm_source_code=.
64. DOJ, “Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin ‘Mixer’ That Laundered Over \$300 Million”, August 18, 2021, <https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million>.



Adam Klauder is a senior director in Guidehouse's Global Investigations and Compliance practice. He is a seasoned compliance executive, attorney, and senior leader with an extensive background in developing overall compliance strategy, directing and coordinating sensitive and high-profile global investigations, and providing strategic guidance on the build-out of corporate compliance functions. Mr. Klauder advises clients in the defence, healthcare, financial services, transportation and logistics, energy and infrastructure, and telecommunications sectors, and is a subject matter expert in compliance matters involving economic sanctions, export controls, anti-corruption, cryptocurrency, and other cross-border regulatory regimes. Prior to joining Guidehouse, Mr. Klauder was a senior global compliance executive at HSBC, serving as Global Head of Sanctions Investigations and Global Investigations Advisor.

Guidehouse
1200 19th Street, NW
Suite 700
Washington, D.C. 20036
USA

Tel: +1 202 481 8371
Email: adam.klauder@guidehouse.com
URL: www.guidehouse.com

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting. We help clients address their toughest challenges with a focus on markets and clients facing transformational change, technology-driven innovation, and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology/analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success. Headquartered in Washington, D.C., the company has more than 7,000 professionals in more than 50 locations. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies.

www.guidehouse.com



The New EU Global Human Rights Sanctions Regime

Rahman Ravelli



Salomé Lemasson

Introduction

On December 7, 2020, the European Union adopted a global sanctions regime against human rights violations and abuses committed worldwide (the “**EU Global Human Rights Sanctions Regime**”).

The recently enacted regime grants the EU more flexibility and efficiency when targeting perpetrators of human rights violations, wherever they are committed. The EU’s foreign policy is, therefore, no longer limited to existing geographical sanctions regimes. Prior to the adoption of this new global regime, the EU decided on financial sanctions, travel bans and other sectoral restrictions on a country-specific basis only (e.g., Belarus, Libya, Myanmar, Syria or Venezuela).¹ The new global regime removes the need for the EU to set up a specific legal framework for each specific case, thus ensuring a rapid response against human rights violations. The new sanctions regime does not replace existing geographic regimes but instead coexists with them.

The EU Global Human Rights Sanctions Regime is in line with the EU Action Plan on Human Rights and Democracy 2020–2024, which was approved by the EU Council on November 17, 2020, whereby the EU committed to developing a new horizontal EU global human rights sanctions regime to tackle serious human rights violations and abuses worldwide.

The EU Global Human Rights Sanctions Regime further underlines that the promotion and protection of human rights is a cornerstone and priority of the EU’s external action. It forms part of a wider political dialogue, and reflects the EU’s determination to enhance its role in addressing serious human rights violations and abuses. As for other international financial sanctions implemented by the EU, in particular restrictive measures, such sanctions are preventive and non-punitive instruments which do not have an economic motivation, but rather aim at fostering a change in policy or activity by the targeted country, administration, entities or individuals.²

Legal Framework

General framework for EU sanctions

The Council of the European Union (“**EU Council**”) has authority to bring restrictive measures against serious human rights violations and abuses under the legal framework of the Common Foreign and Security Policy (“**CFSP**”).

Under Article 29 of the Treaty on European Union (“**TEU**”), the EU Council may adopt sanctions against governments of non-EU countries, non-state entities and individuals. Article 215 of the Treaty on the Functioning of the European Union

(“**TFEU**”) provides that the EU Council may adopt the necessary measures to implement decisions adopted under Article 29 TEU to ensure they are applied uniformly in all Member States.³

Gradual sanctions may be imposed by the EU against third countries, including:⁴

- **Diplomatic Sanctions**, such as expelling diplomats, suspending official visits, suspending cooperation with the EU, etc.; and
- **Economic and Financial Sanctions**, such as embargoes on military goods and restrictive measures such as asset freezes, travel bans and sectoral prohibitions (e.g., restrictions on the import or export of dual use goods).

Sanctions are implemented either at the EU level or national level. Embargoes and travel bans are handled directly by Member States, in compliance with the EU Council’s CFSP decisions. Economic and financial sanctions – such as asset freezes or sectoral prohibitions – are implemented by means of a regulation adopted by the EU Council.⁵

A complex procedure

The implementation of the new EU Global Human Rights Sanctions Regime relies on a complex procedure and various legal tools:

- the EU Council Decision,⁶ proposed by the High Representative (“**HR/VP**”) after discussion with all EU foreign ministers, which sets out the political and legal basis for the new regime; and
- the EU Council Regulation,⁷ which follows a joint proposal from the HR/VP and the EU Commission and complements the EU Council Decision to ensure uniform application of sanctions across the EU.

Both the Decision and Regulation concerning restrictive measures against human rights violations and abuses were adopted on December 7, 2020 by the EU Council, acting by qualified majority pursuant to Article 215 of the TFEU.

Regulations adopted by the EU Council are binding and directly applicable throughout the EU and are under judicial review by the Court of Justice and the General Court in Luxembourg.⁸ As such, they do not need to be transposed into national law. Member States are required, however, to adopt national laws providing for applicable sanctions in case of violation of the restrictive measures imposed by the EU Council.⁹

A Landmark European Initiative

A global sanctions regime

The EU Global Human Rights Sanctions Regime targets

perpetrators – whether individuals or entities, including state and non-state actors – of serious human rights violations or abuses worldwide. It also targets individuals and entities associated with the perpetrators.

The framework for targeted restrictive measures taken under the Global Human Rights Sanctions Regime applies to the following acts:¹⁰

- genocide;
- crimes against humanity; and
- serious human rights violations or abuses, such as torture, slavery, extrajudicial killings, enforced disappearances, arbitrary arrests or detentions.

Other human rights violations or abuses can also fall within the scope of the sanctions regime when they are widespread, systematic or are otherwise of a serious concern as regards the objectives of the EU's common foreign policy. These would include human trafficking, sexual and gender-based violence, violations of freedom of assembly, of religion or of opinion and expression.

Perpetrators of human rights violations and abuses are targeted regardless of where in the world those acts are committed, including when they occur in perpetrators' own states, in other states or across borders.¹¹

EU sanctions create legal obligations for all EU operators, whether inside or outside the EU, and in respect of any business carried out in whole or in part within the EU.¹² However, as underlined by the guidance note published by the EU Commission, the EU Global Human Rights Sanctions Regime does not create obligations for non-EU operators.¹³ In addition to the individual restrictive measures adopted under the EU Global Human Rights Sanctions Regime, EU operators are further required to supply information to and cooperate with competent national authorities and the EU commission to facilitate compliance with the Regulation.¹⁴

Relying on individual restrictive measures

Contrary to past sanctions regimes imposed by the EU, which rely on state-based sanctions, the new EU Global Human Rights Sanctions Regime is individual-based. This shift in approach is aimed at avoiding unintended negative effects on the civilian population. Indeed, while state-based sanctions may induce a deterrent effect on countries guilty of human rights violations, they may unintentionally have negative effects on the social rights and quality of life of innocent civilians living in the targeted state.

As such, the new EU Global Human Rights Sanctions Regime relies on a traditional arsenal of financial sanctions and restrictions on movements targeting perpetrators of human rights violations. There are no arms embargoes or sectoral/economic sanctions, such as import/export bans, in this particular regime.¹⁵

More specifically, sanctions consist of the following individual measures:

- travel ban;
- freezing of funds and economic resources; and
- prohibition of availability of funds and economic resources.

Sanctions are enforced against natural or legal persons, entities or bodies responsible for, providing support to or otherwise involved in serious human rights violations or abuses, as well as those associated with the natural and legal persons, entities and bodies covered.

Exceptions and derogations

All EU sanctions are designed to minimise the risk of unintended consequences for the civilian population. As for other sanctions regimes, exceptions and derogations apply,¹⁶ such as a dedicated humanitarian derogation or asset freeze derogations to satisfy basic needs of designated persons and their dependent family (such as food or medicines). In this respect, the Decision recalls the importance of international human rights law and of the interaction between international human rights law and international humanitarian law when considering the application of targeted restrictive measures.¹⁷

Derogations mean that a restricted or otherwise prohibited action can be carried out only after a Member State's competent authority has granted an authorisation. Exceptions mean that a restriction does not apply when the purpose of the action coincides with the scope of the exemption, which can be carried out without any delay.

Listing process

Under the Global Human Rights Sanctions Regime, the EU Council, acting unanimously upon a proposal from a Member State or from the HR/VP, is responsible for establishing, reviewing and amending the list of sanctioned persons (the “**Consolidated List**”).

Adding sanctioned persons and entities to the Consolidated List must be carried out in compliance with fundamental rights, such as defence rights, as embodied by the TEU and controlled by the ECJ. Sanctions decisions adopted by the EU Council must rely on clear criteria and include an adequate statement of reasons and evidence concerning the adoption of restrictive measures.

To date, the EU Council has added the following individuals and entities to the Consolidated List:

- On March 2, 2021, four Russian individuals were added to the Consolidated List for being responsible for serious human rights violations including arbitrary arrests and detentions, as well as widespread and systemic repression of freedom of peaceful assembly and association, and freedom of opinion and expression in Russia.¹⁸
- On March 22, 2021, 11 individuals and four entities were added to the Consolidated List as a response to the EU's deep concerns about serious human rights violations such as torture, extrajudicial killings, enforced disappearances or systematic use of forced labour committed by the targeted entities in China, Eritrea, Libya, North Korea, Russia and South Sudan.¹⁹

These sanctions supplement the 200+ individuals and entities already sanctioned for human rights violations or abuses pursuant to the EU's existing geographical sanctions regimes.

Mirroring Other Sanctions Regimes

The US Global Magnitsky Act

According to the HR/VP Josepp Borrel, the EU Global Human Rights Sanctions Regime is directly inspired by the Magnitsky Act, which was passed by the US Congress and signed into law by President Barack Obama in December 2012.²⁰ The Magnitsky Act was adopted in the aftermath of the death of the Russian lawyer Sergei Magnitsky while imprisoned following his investigations into allegations of tax fraud potentially targeting high-ranking Russian officials.

Initially targeting human rights violations committed in Russia only, the Magnitsky Act was extended in 2016 to target any perpetrator of human rights violations globally, as well as corruption. It is now commonly referred to as the Global Magnitsky Act.

Other Human Rights Sanctions Regimes

Other countries have adopted similar sanctions regimes targeting human rights violations, including Canada, Estonia, Latvia, Lithuania and the United Kingdom.

Following its departure from the EU, the UK adopted the Global Human Rights Sanctions Regulation in July 2020, allowing the country to sanction “*perpetrators of the worst human rights abuses*” globally. The UK’s sanctions regime was introduced under the UK Sanctions and Anti-Money Laundering Act of 2018, the new legislative framework implemented to allow the UK to continue implementing pre-existing EU sanctions throughout the transition period of its exit from the Union. As is the case with the Global Magnitsky Act, the scope of the UK’s sanctions regime covers corruption, contrary to the EU Global Human Rights Sanctions Regime.

Australia also announced that it is considering whether to introduce similar sanctions against gross human rights abusers, irrespective of where in the world their conduct occurs. A parliamentary inquiry was launched on this topic in 2019 by the Australian Joint Standing Committee on Foreign Affairs, Defence and Trade, which issued its report on December 7, 2020.²¹ The conclusions of the parliamentary inquiry recommend that the Australian Government enacts stand-alone targeted sanctions legislation to address human rights violations and corruption, similar to the US Magnitsky Act of 2012.²²

Towards the expansion of the EU Global Human Rights Sanctions Regime to corruption?

The question is now being debated at EU-level of whether to follow the example of the US Magnitsky Act and include corruption in the list of sanctioned offences. In June 2021, the EU’s Foreign Affairs Committee adopted a resolution welcoming the EU Global Human Rights Sanctions Regime while calling for corruption to be included as a punishable offence.

So far, the philosophy of the fight against corruption as carried out by the international community has been to target and punish individuals and entities that bribe, not the public officials being bribed. Economic sanctions would have the benefit of enhancing the tools available to deter corruption by targeting corrupt public officials, who would then be added to the Consolidated List.

However, criticism has been voiced against such an expansion.²³ Critics argue that adding corruption to the EU Global Human Rights Sanctions Regime would be inefficient. Corruption would not be tackled by adding corrupt officials to the list of sanctioned individuals, given that the designation process is the result of a long and cumbersome political and diplomatic process.

But above all, critics warn against such an approach as this would result in dodging the role of the police and judicial authority. Indeed, adding corrupt public officials to the list of designated individuals would raise thorny questions of how to determine whether allegations of corruption are established, according to what standard of proof and based on which procedural framework parallel to each Member State’s established criminal justice system. If listing were to occur after a final and binding judicial decision were to be rendered, this raises the question of the deterrence effect of such a listing.

Some voices raise the issue that adding corruption to the scope of the EU Global Human Rights Sanctions Regime would belittle the emergence of European criminal law, for which the implementation of the European Prosecution Office has been a critical first step. In a nutshell, critics argue that international economic sanctions should remain an alternative to armed conflict but not to criminal justice.

Endnotes

1. The long and complex road towards an EU Global Human Rights Sanctions Regime, <https://eeas.europa.eu>.
2. EU Commission (Updated) Sanctions Guidelines, May 4, 2018.
3. General Framework for EU Sanctions, <https://eur-lex.europa.eu>.
4. General Framework for EU Sanctions, <https://eur-lex.europa.eu>.
5. EU Commission (Updated) Sanctions Guidelines, May 4, 2018.
6. Council Decision (CFSP) 2020/1999 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses.
7. Council Regulation (EU) 2020/1998 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses.
8. EU Commission (Updated) Sanctions Guidelines, May 4, 2018.
9. EU Commission (Updated) Sanctions Guidelines, May 4, 2018.
10. Article 1, Council Decision (CFSP) 2020/1999 of December 7, 2020.
11. Questions and Answers: EU Global Human Rights Sanctions Regime, December 7, 2020.
12. Article 19, Council Regulation (EU) 2020/1998 of December 7, 2020.
13. Commission Guidance Note on the Implementation of Certain Provisions of Council Regulation (EU) 2020/1998.
14. Article 9, Council Regulation (EU) 2020/1998 of December 7, 2020.
15. Commission Guidance Note on the Implementation of Certain Provisions of Council Regulation (EU) 2020/1998.
16. Articles 4 to 7, Council Regulation (EU) 2020/1998 of December 7, 2020.
17. Para. 4, Council Decision (CFSP) 2020/1999 of December 7, 2020.
18. Council Implementing Regulation (EU) 2021/371 of March 2, 2021 implementing Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses.
19. Council Decision (CFSP) 2021/481 of March 22, 2021 amending Decision (CFSP) 2020/1999 concerning restrictive measures against serious human rights violations and abuses.
20. Russia and Moldova Jackson-Vanik Repeal and Sergei Magnitsky rule of law Accountability Act of 2012.
21. Criminality, corruption and impunity: Should Australia join the Global Magnitsky movement? An inquiry into targeted sanctions to address human rights abuses, Australia’s Joint Standing Committee on Foreign Affairs, Defence and Trade.
22. Cf. recommendation No. 1.
23. *Le Monde, Combattre la corruption par les sanctions économiques internationales est une fausse bonne idée*, Emmanuel Breen, July 19, 2021.



Salomé Lemasson leads Rahman Ravelli's EU Business Crime and Regulatory Practice Group.

Admitted to practise in France and Germany, she has extensive experience of representing major corporations and individuals in high-stakes national and multinational criminal proceedings, cross-border litigation and regulatory investigations.

Her workload at any given time includes sanctions investigations, corporate tax fraud and corruption allegations, and a wide variety of multi-lateral development bank (MDB) cases related to corruption, collusion and fraudulent practices. She is an accomplished defence lawyer who has worked on some of Europe's most challenging and significant white-collar crime investigations.

Salomé has in-depth experience of both conducting internal investigations for major corporates and negotiating settlement agreements for them. She played a senior role in internal investigations conducted into several major motor vehicle manufacturers' emissions practices and into leading pharmaceutical companies' COVID-19 vaccine manufacturing processes.

With extensive deferred prosecution agreement experience, her track record includes helping a global technology company secure a €500 million DPA with the French Financial Prosecutor in relation to tax fraud allegations.

Rahman Ravelli
36 Whitefriars Street
London, EC4Y 8BQ
United Kingdom

Tel: +44 208 106 7438
Email: salome.lemasson@rahmanravelli.co.uk
URL: www.rahmanravelli.co.uk

Rahman Ravelli's depth of experience, its widely-acknowledged national and international expertise and its legal successes have earned it a reputation second to none.

It is a reputation for managing the largest and most complex multinational and multi-agency investigations into sanctions, serious and corporate fraud, white-collar crime, bribery and corruption, regulatory matters, complex crime and market abuse.

Handling some of the most significant sanctions cases discreetly and intelligently, Rahman Ravelli is one of the UK's most prominent legal firms when it comes to managing all aspects of criminal and regulatory defence and dealing with UK and worldwide agencies. Operating from locations across Europe, it is in increasing demand to provide major corporates, other organisations and senior individuals with strategic international advice.

The Legal 500 Guide called it "an exceptional firm with exceptional people" while *Chambers* UK Guide said it was "[a]bsolutely outstanding. An impressive team with real depth".

www.rahmanravelli.co.uk

RAHMAN RAVELLI | solicitors

Annual Developments in EU Sanctions Litigation



Sebastiaan Bennink



Shanne Verkerk



Sarah Reilly

BenninkAmar Advocaten

Annual Developments in EU Sanctions Litigation

2021 saw European Union (“EU”) sanctions taken against individuals and entities under the current sanctions regimes, but also the first listings based on the new EU Global Human Rights Sanctions Regime.¹ On 22 March 2021, the Council of the EU (the “Council”) decided to list the first 15 individuals and entities under this regime, considered responsible for, involved in or associated with, serious human rights violations and abuses worldwide. Also on 22 March 2021, following the military coup in Myanmar, the Council imposed restrictive measures on those considered responsible for undermining the country’s democracy and rule of law.² In June 2021, following the orchestrated landing of an aircraft in Minsk and the ensuing detention of a Belarusian journalist, the EU introduced new restrictive measures against the national regime in an effort to reduce internal repression of civil society and democratic opposition.³

While sanctions are topical and well-publicised, less is written on the challenges in relation to them. Targeted individuals and entities attempt to challenge sanctions or annul their listings, as the restrictive measures that follow from these travel bans and freezing of funds significantly curtail their freedom of movement and impact their livelihood. The increase in sanctions also leads to questions on a national level with respect to enforcement and consequences for individuals and entities. As a result, procedural and substantive issues, often triggered by national requests for preliminary rulings or challenges of Council listings, are brought before the Court of Justice of the European Union, and more specifically the General Court (“General Court”) or the Court of Justice (“ECJ”). If the ECJ decides that an Opinion of the Advocate General (“AG”) is necessary, such an opinion will also be provided.

This chapter will focus on some of the more conspicuous cases of 2021. These range from the first ECJ judgment on the admissibility of a third state appeal, to listing annulment requests bringing to the fore discussions around notification, grounds for listing and judicial protection. 2021 was also a year during which AGs gave their opinion on how to interpret certain sanctions issues, e.g. the objective and implications of the EU blocking statute and the scope of asset freezes.

Admissibility of a Third State to Challenge a Sanction Regime

For a sanctioned party to be removed from an EU sanctions list, it must submit a substantiated request to the Council to reconsider its listing decision, challenge the Council’s decision before the General Court and, if necessary, appeal this decision before the ECJ. Article 263 paragraph 4 of the Treaty of the Functioning of the European Union (“TFEU”)⁴ allows “any natural or legal person” to request the annulment of an EU act, provided that the contested act is addressed to them specifically or is of direct and individual concern to them.

The question of whether third (non-EU) states are entitled to institute proceedings challenging sanctions before the EU judiciary came to the fore in AG Hogan’s Opinion in *Bolivarian Republic of Venezuela v Council*, delivered on 20 January 2021 and the related judgment by the ECJ, rendered on 22 June 2021.⁵

In 2018, Venezuela initiated proceedings before the General Court, challenging certain restrictive measures laid down in the EU sanctions regime against Venezuela, i.e. Council Regulation (EU) 2017/2063.⁶ The Council argued the inadmissibility of the challenge, stating that Venezuela had no legal interest in bringing proceedings, that it was not directly concerned by the provisions of the sanctions regime and that it was not a “natural or legal person” under Article 263 TFEU. The General Court dismissed the action as inadmissible, ruling that the sanctions regime did not directly concern Venezuela, without looking at the other grounds for inadmissibility.

When Venezuela appealed the decision before the ECJ, AG Hogan opinionated that the latter should rule that the General Court erred in its application of the law on inadmissibility, that the General Court had been “highly artificial” and “unduly formalistic”,⁷ and that it should have adjudicated on all remaining admissibility issues in the annulment proceedings and on the merits. The ECJ followed the AG’s reasoning, setting aside the judgment of the General Court and referring the case back for judgment on the merits.

A non-restrictive understanding of legal person

In determining whether Venezuela was to be regarded as a “legal person” under Article 263 TFEU, the Member States were also

asked for their opinion. Unsurprisingly, the Council argued that considering third states as legal persons would lead to EU courts being used as a back door for resolving international disputes among subjects of international law and restricting the EU in the conduct of its policies and international relations.⁸ Some Member States shared this reasoning, while others argued that third states were to be considered as legal persons, as considering otherwise would prevent them from protecting their interests, constituting a restrictive interpretation of the rule of law.⁹

The ECJ found that the term “legal person” could not be interpreted restrictively, as it did not follow from the wording, context and objective of Article 263 TFEU or from other provisions of EU primary law that certain legal persons could not avail themselves of the possibility of instituting legal proceedings before the EU courts.¹⁰ The ECJ also found that it followed from the case law that private and public legal persons could bring proceedings under Article 263 TFEU.¹¹ Considering the principles of effective judicial review and rule of law, the ECJ concluded that a third state had standing to bring proceedings as a “legal person” under Article 263 TFEU.

An immediate and automatic effect of prohibitions amounts to direct concern

The ECJ then looked to establish whether the restrictive measures of the sanctions regime were of “direct concern” to Venezuela under Article 263 TFEU.

While the Council argued, *inter alia*, that it was clear that Venezuela was not addressed directly by the Regulation that targeted “EU economic operators”,¹² the ECJ found that Regulation 2017/2063 had in fact the effect of immediately and automatically applying the prohibitions set out in its provisions. As this “prevent[ed] the Bolivarian Republic of Venezuela from obtaining numerous goods and services” and “directly affect[ed] the legal situation of that State”,¹³ the ECJ thereby concluded that the General Court had erred in law in considering that the restrictive measures at issue did not directly affect Venezuela.¹⁴

The rejected grounds of inadmissibility brought by the Council

The ECJ addressed the two further grounds of inadmissibility argued by the Council,¹⁵ rejecting them both.

In determining whether Venezuela had an interest in instituting proceedings, the ECJ explained that such an interest presupposes that the annulment of the contested act must result in procuring an advantage for the natural or legal person bringing the action. The ECJ concluded that considering that the prohibitions in the Regulation were liable to harm namely the economic interests of Venezuela, their annulment could procure an advantage.¹⁶ The ECJ thereby rejected this ground of inadmissibility.

The ECJ then addressed the second of the two cumulative criteria necessary to show direct concern: i) that the restrictive measures must directly affect the legal situation of the person; and ii) leave no discretion to the addressees who must implement them. While the Council argued that Regulation 2017/2063 necessarily entailed the adoption of intermediate rules, its provisions setting out a system of prior authorisation by the competent authorities of the Member States, the ECJ found that from the wording of the Regulation, the prohibitions applied without leaving any discretion to the addressees responsible for implementing them.¹⁷

Interestingly, this case demonstrates that restrictive measures under a sanctions regime can be of direct concern to or affect third states, despite not being addressed to the latter. This is justified, *inter alia*, on the fact that restrictive measures are directly applicable in Member States without prior implementation into national law and that they have the effect of potentially restricting third states from obtaining goods and services. Moreover, this case shows that the understanding of any “legal person” should be interpreted non-restrictively, considering the principles of effective judicial review and rule of law. It shows that the context and objectives pursued by the EU law of which Article 263 TFEU is a part are to be considered in the interpretation of this provision.

Admissibility of an Individual to Challenge a Listing for Mere Association with a Targeted Regime

Much of the sanctions litigation of recent years relates to listing annulment requests and 2021 was no exception. Many of these requests have been successful – the EU courts finding that the Council had insufficiently investigated the information on which the listings were based or had failed to provide evidence for the listings.¹⁸

The question of whether an individual is entitled to challenge the Council’s decision to maintain their name on a listing on the basis of their association with a repressive regime and whether the Council has a duty to notify them of this decision came to the fore in *Aisha Muammer Mohamed El-Qaddafi v Council*, in which the judgment was rendered by the General Court on 21 April 2021.¹⁹

The applicant, Aisha Qaddafi, is a Libyan national and the daughter of former Libyan leader Muammer Qaddafi, the leader of Libya from 1969, when he seized power in a military coup, to his assassination in 2011. For reasons of family ties and “closeness of association” with the regime, Aisha Qaddafi’s name was included on the United Nations Security Council Resolution 1970 (2011) (the “UN Resolution”).²⁰ The UN Resolution introduced restrictive measures against Libya and against persons and entities involved in serious human rights abuses, by involvement in attacks on civilian populations in violation of international law. Following this, in February and March 2011, the Council adopted the 2011 acts²¹ concerning restrictive measures in relation to Libya and including Aisha Qaddafi’s name on their related annexes. In 2017 and 2020, the Council adopted the 2017 acts²² and the 2020 acts²³ that maintained the applicant’s name on the lists in their respective annexes, without any amendment to the statement of reasons for her designation. Aisha Qaddafi sought the annulment of the 2017 and 2020 acts (together, the “Contested Acts”), as their restrictive measures consisted of a travel ban and an asset freeze, prejudicial to her daily life.

An implied obligation to notify the listed person of a renewed listing

The Council argued the inadmissibility of Aisha Qaddafi’s claim based on Article 263 paragraph 6 TFEU²⁴ – which provides for a two-month delay to institute proceedings from the publication or notification of the restrictive measure or, in the absence thereof, from the day on which it came to the knowledge of the claimant – on account of the claim being time-barred. Further, the Council argued that it was under no express obligation under the EU Libya sanctions regime to notify the Contested Acts to listed persons.²⁵ It contended that the point at which an act

comes to the knowledge of a listed person is the starting point of the two-month delay only when the contested act had neither been published, whereas the Contested Acts had been published in the Official Journal.²⁶ Aisha Qaddafi argued that her action was not time-barred, as she had lodged her action within two months from the notification of the Contested Acts by respective letters from the Court Registry. Further, she argued that the Council was under the obligation to notify listed persons of decisions on listings.²⁷

The General Court, while recognising that the EU Libya sanctions regime did not impose on the Council an express obligation to notify, sided with the applicant on admissibility.²⁸ It referred to *Mayaleh v Council*²⁹ that stated that the notifying obligation stems from the principle of effective judicial protection, meaning that the EU institution that adopts or maintains individual restrictive measures is bound to communicate the grounds – and this at the moment of adoption or as soon as possible after, in order to allow for potential challenges.³⁰ Referring also to *Gbagbo and Others v Council*,³¹ the Court added that the Council did not have the discretion of the means of communication to the listed persons subject to restrictive measures.³² The General Court concluded that it is only when it is impossible to communicate an act to the person concerned, e.g. when there is no address available or that direct notification fails, that the publication in the Official Journal constitutes the starting point for the period in which an annulment action can be brought, so as not to hinder individuals' right to access EU courts. Otherwise, on account of the lack of foreseeability of the amendments to listings, individuals would have to continually verify the Official Journal.³³ The General Court noted that it was not apparent that the Contested Acts had come to Aisha Qaddafi's knowledge prior to the Court Registry letters, which led it to conclude that Aisha Qaddafi was not time-barred from bringing an annulment action in relation to the Contested Acts.³⁴

A statement of reasons making intelligible the restrictive measures

On the merits, Aisha Qaddafi argued, *inter alia*, a failure to disclose a lawful basis and a statement of reasons for maintaining her name on the lists at issue and disproportionate infringement of her fundamental rights.³⁵

The General Court stressed that the obligation to state the reasons for a listing was a corollary of the principle of respect for the rights of defence. Referring, *inter alia*, to *Council v Bank Mellat and Kadhafi Al Dam v Council*, it found that the statement of reasons must identify the individual, specific and concrete reasons why the competent authorities considered restrictive measures necessary for the person concerned, allowing for the person's understanding.³⁶ The General Court noted that Aisha Qaddafi had been listed pursuant to the UN Resolution due to her association with the Muammar Qaddafi's regime, and that the Council had informed that it was witness to her public statements calling for the overthrow of the Libyan authorities and her father's revenge. The Court thereby concluded that Aisha Qaddafi was, on this basis, in a position to comprehend the context and scope of the restrictive measures and to prepare to challenge them and thereby rejected this part of the plea.³⁷

A mere association is not a solid factual basis for listing

On the absence of factual basis for maintaining her name on the list, the General Court recalled the effectiveness of the judicial review guaranteed by Article 47 of the Charter of Fundamental Rights of

the European Union (the “Charter”). Such a review requires that the EU courts ensure that decisions by which restrictive measures were adopted or maintained and that affect persons individually are taken on a sufficiently solid factual basis. Referring, *inter alia*, to *Commission and Others v Kadi*,³⁸ the General Court noted that if such a decision is challenged, the competent EU authority has the duty to establish that the reasons, *a minima* one reason, relied on against the person concerned are substantiated – the listed person does not have the duty to show evidence of the negative.³⁹

The General Court agreed with the Council that the entry of Aisha Qaddafi's name on the Contested Acts on account of being the “daughter of Muammar Qadhafi” and her “closeness of association with [his] regime” was not challenged in good time. However, the General Court found that it was not because the Council was entitled to refer to the UN Resolution's statement of reasons that it was relieved of its obligation to demonstrate a sufficiently solid factual basis for the maintaining of Aisha Qaddafi's name on the lists.⁴⁰ On this, the General Court noted that the Council had not showed evidence of the risk that Aisha Qaddafi posed to international peace and security in Libya, whereas she had ceased to reside in the country and was not participating in Libyan political life. The Court concluded that the Council had no factual basis to justify the retention of Aisha Qaddafi's name on the Contested Acts, which were thereby annulled in so far as they concerned the applicant.⁴¹

Interestingly in this case, Aisha Qaddafi was not listed for having committed serious human rights violations or abuses in Libya herself, but solely for her family ties with Muammar Qaddafi and her closeness to his regime. Under the EU Libya sanctions regime, the listing criteria specifically requires the targeted person to, besides mere association, pose a continued risk to the peace, stability or security of Libya, or the successful completion of its political transition. The necessity to meet this double-criteria *de facto* explains the annulment of her listing. However, it is good to note that not all sanctions regimes provide for such additional listing criteria. For example, the new EU Global Human Rights Sanctions Regime allows for persons to be listed on the basis of mere association with persons considered responsible for human rights violations. It thereby remains to be seen if these persons will be successful in challenging their listing in the same way as Aisha Qaddafi.

Moreover, this case poses the more general question of whether a person's association with a person targeted by the sanctions regime should constitute a listing criteria at all. Although the validity of such a listing was not challenged in this decision, as the challenge was time-barred, the legitimacy of this ground is somewhat questionable. Prior cases on this topic also fail to provide an answer to this question. For example, in *Oleksandr Viktorovych Yanukovich v Council*, the son of former Ukrainian president Yanukovich, unsuccessfully challenged his listing, as he himself was subject to criminal proceedings, in themselves considered a solid factual basis for a listing.⁴² In *Tay Za v. Council*, the son of a businessman who benefitted from the sanctioned military regime of Myanmar successfully challenged its listing – the ECJ finding that the presumption that the family of the businessman benefitted from his functions and thereby also from the economic policies of the government was insufficient to link Tay Za to the sanctioned Myanmar military regime.⁴³ These different outcomes can be explained by the extent of the association of the listed applicant with the sanctioned person, but also perhaps and more likely so, by a *de facto* analysis of the circumstances of each case. In any event, it appears that the decision to list an individual should *a minima* be based on a sufficiently solid factual basis in order for the specific listing criteria to be met. It remains up to future case law to reveal what exactly constitutes a sufficiently solid factual basis for the listing criteria of mere association to be met.

The Weight to Attribute to the EU Blocking Statute *versus* US Secondary Sanctions

The multiplication of sanctions regimes around the world poses the question of the applicability of their extraterritorial reach, as well as the manner in which businesses must reckon with occasional contradictory legal frameworks.

For instance, the US has had a long-standing practice of imposing sanctions against individuals, entities and countries. While these sanctions apply mainly to US persons and non-US persons within US jurisdiction who trade or invest with those concerned (“**primary sanctions**”), some sanctions also target activities beyond US jurisdiction and can target non-US companies for trading with those concerned by US sanctions (“**secondary sanctions**”). These attempts at US extraterritorial jurisdiction have been criticised at EU level and in an effort to mitigate them, the EU blocking statute⁴⁴ was adopted, its provisions prohibiting EU enterprises from complying with US measures.

The issue of EU enterprises’ compliance with US secondary sanctions and the weight to attribute to the EU blocking statute came to the fore in AG Hogan’s Opinion in *Bank Melli Iran, Aktiengesellschaft nach iranischem Recht v Telekom Deutschland GmbH*, delivered on 12 May 2021.⁴⁵

By way of context, former US President Donald Trump decided in May 2018, to have the US withdraw from the Iranian nuclear deal⁴⁶ and reactivate the Iranian Transactions and Sanctions Regulations against Iranian entities. This suddenly posed significant difficulties for EU enterprises, such as Telekom Deutschland GmbH, which had business in Iran or with Iranian entities and were thereby suddenly exposing themselves to US secondary sanctions. In order to prevent the effects of these reactivated US sanctions, the EU added the US legislation related to the Iran sanctions regime to the foreign legislation covered by the EU blocking statute, but this fell short of reassuring some EU enterprises that they would not be subject to US secondary sanctions.

Following the reactivation of US sanctions, Bank Melli Iran (“**Bank Melli**”) was once again placed on a list of sanctions prepared by the US Office of Foreign Asset Control (“**OFAC**”) Specially Designated Nationals and Blocked Persons List (“**SDN List**”).⁴⁷ As a result, Telekom Deutschland GmbH (“**Telekom Deutschland**”), a telecommunication provider and subsidiary of Deutsche Telekom that generates approximately 50% of its turnover in the US, terminated all contracts with Bank Melli’s German branch.

This was prejudicial to Bank Melli’s communication structures as indispensable to its business activities. Bank Melli appealed the decision before the Hanseatic Higher Regional Court (Hamburg, Germany), arguing that the termination was to be held invalid as it was solely motivated by Telekom Deutschland’s intent to comply with US secondary sanctions prohibiting non-US entities from contracting with US-sanctioned Iranian entities, whereas Article 5 paragraph 1 of the EU blocking statute prohibits EU undertakings from complying with such extraterritorial US measures.⁴⁸ In turn, Telekom Deutschland, argued that that same article of the EU blocking statute did not change its ordinary right to terminate such a contract without giving reasons for this action.

By way of request for a preliminary ruling, the German court asked the ECJ for its interpretation of the EU blocking statute. More specifically, it asked the following questions:

- whether Article 5 paragraph 1 of the EU blocking statute only applied where the EU enterprise is issued with a US official court order or whether mere intended compliance with US secondary sanctions sufficed;

- whether that same article prevented a party from terminating a continuing obligation with an OFAC SDN, including where termination was motivated by compliance with US sanctions, without the need to give a reason for termination;
- whether ordinary termination in breach of the same article was necessarily ineffective or whether other alternative penalties be imposed; and
- whether the same article could apply considering the freedom to conduct business of Article 16 of the Charter and the principle of proportionality of Article 52 of the Charter and the exemption provided by Article 5 paragraph of the EU blocking statute allowing EU enterprises to comply with foreign legislation covered by the statute, should non-compliance “seriously damage their interests” and in the event where maintaining the business relationship with the listed contracting party would expose the EU operator to considerable economic losses on the US market (in this case: 50% of group turnover).⁴⁹

As a preliminary note, the AG stated that the tensions between the two legal regimes lead to “*European companies finding themselves facing impossible – and quite unfair – dilemmas brought about by the application of two different and directly opposing legal regimes*”. He pondered that these dilemmas and the lack of guidance on important legal issues arising from the EU blocking statute were such that the “*EU legislature might with advantage review the manner in which that statute presently operates*”. He added, however, that the review of the statute was a matter of law and not of the Court.⁵⁰

On the first question, the AG then found that the EU blocking statute made clear from its wording, context and objectives that the general prohibition it contained in its Article 5 para. 1 for EU entities to comply with third country legislation providing for secondary sanctions applies even when such entities comply with that legislation without having been compelled to do so by a foreign administrative or judicial authority. Mere intent to comply should suffice.⁵¹

On the second question, the AG noted that German contract law does allow for the termination of contracts without having to motivate the termination. However, the AG found that an EU enterprise attempting to terminate a contract with an Iranian entity subject to the US sanctions must demonstrate to the satisfaction of the national court that it did not do so only to comply with those sanctions – the EU blocking statute held to impose an obligation to justify the termination of a business relationship with a person subject to primary sanctions. The AG recognised this right of action to enforce Article 5 paragraph 1 of the EU blocking statute with reluctance, admitting that the collateral consequence of this interpretation is that third country entities targeted by the US sanctions could obtain the benefit of the EU blocking statute at the expense of an EU entity. The AG stressed that this was not the intent of the EU blocking statute, which in fact looks to protect EU enterprises against legislation contrary to national sovereignty and international law. Pointing to the uncompromising language of the EU blocking statute and the policy objectives behind the latter, the AG nevertheless concluded that denying such a right of action would amount to relying on the willingness of Member States to comply with the EU blocking statute and could lead to the latter being undermined.⁵²

Considering that Bank Melli Iran and Telekom Deutschland were already in a contractual relationship and that their business activity has remained the same, the AG noted that Telekom Deutschland had to demonstrate an objective reason, other than the fact that Bank Melli was subject to primary sanctions, warranting the contractual termination and that the national German court had to verify these grounds.⁵³ This being said,

the AG noted that economic operators can justify their refusal to deal with Iranian entities by invoking their commitment to a coherent and systematic corporate social responsibility policy.⁵⁴

On the third and fourth questions, the AG found that should the EU enterprise violate the EU blocking statute prohibition to comply with US secondary sanction legislation, the national court seized by its contracting party subject to US primary sanctions would be required to order the EU enterprise to maintain their contractual relationship. The national court is to issue this injunction measure despite the possible infringement of the freedom to conduct business and the risk of an EU enterprise being severely penalised by the foreign authorities as a result.⁵⁵

A judgment of the Dutch court of The Hague from June 2019 showed a similar line of reasoning where the Dutch-incorporated company Exact wanted to terminate its contract with PAM, a Cuban incorporated entity.⁵⁶ The shares of Exact had been acquired by KKR, a US-incorporated company, which had ordered Exact to terminate all relations with Cuba on account of Cuban sanctions under the US Helms Burton Act. Exact pleaded *force majeure* before the Dutch court, arguing that maintaining contractual relations with the Cuban entity would entail major liability consequences. The Dutch court dismissed this argument, ruling that any possible criminal or financial consequence arising out of the continuation of the underlying contract comes at the risk of Exact, as Exact agreed to the acquisition and the termination was a shareholder decision. The Dutch court found that Exact had failed to argue solid grounds for the termination and that it was at risk of possibly violating the EU blocking statute if it complied with the Helms Burton Act.

The AG's Opinion in Bank Melli highlights that it is still very questionable, as it has been argued before, should the EU blocking statute provide for safeguards for EU entities who are dealing with these kind of issues. The AG concludes to the blunt nature of the EU blocking statute, which has the adverse consequence of penalising EU enterprises such as Telekom Deutschland – an implication that can only be resolved by the EU legislature reviewing the wording of the statute.⁵⁷

Some Additional Cases in Short

Although this chapter could not showcase all the interesting cases brought before the EU courts in 2021, a few more are described in short.

On 17 June 2021, AG Pitruzzella delivered an opinion⁵⁸ following a request for preliminary ruling by the *Cour de cassation* (Paris, France) in a dispute between Bank Sepah, an Iranian bank that saw its assets frozen, and two of its creditors.⁵⁹ The question arose as to whether – under Council Regulation (EC) No 423/2007 and Council Regulation (EU) No 961/2010⁶⁰ – the creditors could implement measures such as a judicial lien or a preventive attachment in relation to frozen assets of the listed bank, without prior authorisation from the competent national authority. The AG found that it followed from the broadly defined wording, context and objective of the Regulations that freezing of funds and economic resources also covered measures with no earmarking effect,⁶¹ since the definitions did not presuppose a change of ownership or possession of the assets concerned.⁶² Consequently, the AG concluded that the Regulations should be interpreted as also requiring prior authorisation from the competent national authority for measures with no earmarking effect in relation to the frozen funds, in order for them to be implemented. The AG added that it was for the referring court to determine whether the measures of judicial lien or preventive attachment provided for in the French Code of Civil Enforcement Proceedings were in fact measures with no earmarking effect.⁶³ This Opinion thereby clarified the scope

of freezing of funds and economic resources and showed the far-reaching implications of these measures.

Also in 2021, several listings were challenged. Since 2015, the tendency of successful annulment requests appears to have been reversed, the EU courts rejecting the annulment requests more often than not.⁶⁴ For example, in *Council v Kurdistan Workers' Party*, the ECJ ruled that the Council had sufficiently detailed the reasons for the listing of the PKK on the terrorism list.⁶⁵ According to doctrine, the reason behind the reversal of this tendency is not so much that the Council is producing more or better evidence, but that the EU courts are willing to accept legal constructions for listings, such as the substantiation of one reason as a solid factual basis or presumptions based on inferences.⁶⁶ This being said, other cases in 2021 show that the EU courts, despite their acceptance of one substantiated reason, do not forgo their duty to remind the Council to remain critical in its collection and demonstration of evidence justifying a listing. For example, in *Viktor Fedorovych Yanukovych v Council*, the General Court ruled that by basing the listing of the former president of Ukraine on the criminal proceedings against him for embezzlement of state funds, the Council had not satisfied itself that the Ukrainian authorities complied with the applicant's right to a defence and effective judicial protection.⁶⁷ In *Sayed Shamsuddin Borborudi v Council*, the General Court found that the Council had failed to demonstrate that the applicant was Deputy Head of the [United Nations] designated Atomic Energy Organisation of Iran, or was involved in Iran's nuclear programme.⁶⁸ In any event, these cases demonstrate that the Council must improve its investigation and collection of evidence and its communication of the statement of reasons in relation to listings – and this, in order to strengthen the credibility of listings under the sanctions regimes.

Endnotes

1. Council Regulation (EU) 2020/1998 of 7 December 2020 concerning restrictive measures against serious human rights violations and abuses.
2. Council Regulation (EU) No 401/2013 of 2 May 2013 concerning restrictive measures in respect of Myanmar/Burma and repealing Regulation (EC) No 194/2008; Council Decision 2013/184/CFSP of 22 April 2013 concerning restrictive measures against Myanmar/Burma and repealing Decision 2010/232/CFSP.
3. Council Regulation (EU) 2021/1030 of 24 June 2021 amending Regulation (EC) No 765/2006 concerning restrictive measures in respect of Belarus; Council Decision (CFSP) 2021/1031 of 24 June 2021 amending Council Decision 2012/642/CFSP concerning restrictive measures in view of the situation in Belarus.
4. Article 263 paragraph 4, Treaty on the Functioning of the European Union, 2012/C 326/01, 26 October 2021.
5. Case C-872/19 P, *Bolivarian Republic of Venezuela v Council*, Opinion of Advocate General Hogan, 20 January 2021; Case C-827/19 P, *Bolivarian Republic of Venezuela v Council*, ECLI:EU:C:2021:507, 22 June 2021.
6. Council Regulation (EU) 2017/2063 of 13 November 2017 concerning restrictive measures in view of the situation in Venezuela.
7. Case C-872/19 P, *Bolivarian Republic of Venezuela v Council*, Opinion of Advocate General Hogan, 20 January 2021, Para. 109.
8. Case C-827/19 P, *Bolivarian Republic of Venezuela v Council*, ECLI:EU:C:2021:507, 22 June 2021, Paras 28–29.
9. *Id.*, Paras 30–36.
10. *Id.*, Para. 44.

11. *Id.*, Para. 46.
12. *Id.*, Para. 57.
13. *Id.*, Para. 69.
14. *Id.*, Para. 73.
15. *Id.*, Para. 77.
16. *Id.*, Paras 81–85.
17. *Id.*, Para. 90.
18. See N. Zelyova, ‘Restrictive measures - sanctions compliance, implementation and judicial review challenges in the common foreign and security policy of the European Union’, *ERA Forum*, 2021; E. Chachko, ‘Foreign Affairs in Court: Lessons from CJEU Targeted Sanctions Jurisprudence’, *The Yale Journal of International Law*, 2019, Vol. 44; L.A. Verheyen, ‘Challenging the Validity of EU Sanctions Imposed on Individuals: Lessons from the Case Law of the CJEU’, 2019, dissertation, Ghent University; C. Eckes, ‘The Law and Practice of EU Sanctions’. In S. Blockmans, & P. Koutrakos (Eds.), *Research Handbook on the EU’s Common Foreign and Security Policy*, 2018.
19. Case T322/19, *Aisha Muammer Mohamed El-Qaddafi v Council*, ECLI:EU:T:2021:206, 21 April 2021.
20. United Nations Security Council, Resolution S/RES/1970 (2011), 26 February 2011.
21. Decision 2011/137/CFSP concerning restrictive measures in view of the situation in Libya; Regulation (EU) No 204/2011 concerning restrictive measures in view of the situation in Libya.
22. Implementing Decision (CFSP) 2017/497 implementing Decision 2015/1333; implementing Regulation (EU) 2017/489 implementing Article 21(5) of Regulation 2016/44.
23. Implementing Decision (CFSP) 2020/374 implementing Decision 2015/1333; implementing Regulation (EU) 2020/371 implementing Article 21(5) of Regulation 2016/44.
24. Article 263 paragraph 6, Treaty on the Functioning of the European Union, 2012/C 326/01, 26 October 2021.
25. Council Decision (CFSP) 2015/1333 concerning restrictive measures in view of the situation in Libya; Council Regulation (EU) 2016/44 concerning restrictive measures in view of the situation in Libya, repealing the 2011 acts and still including the applicant in the lists of their respective Annexes.
26. Case T322/19, *Aisha Muammer Mohamed El-Qaddafi v Council*, ECLI:EU:T:2021:206, 21 April 2021, Paras 44–45.
27. *Id.*, Paras 47–48.
28. *Id.*, Paras 47–48.
29. Case T-307/12 and Case T-408/13, *Mayaleh v Council*, EU:T:2014:926, 5 November 2014, Para. 57.
30. Case T322/19, *Aisha Muammer Mohamed El-Qaddafi v Council*, ECLI:EU:T:2021:206, 21 April 2021, Para. 51.
31. Case C-478/11 P, *Gbagbo and Others v Council*, EU:C:2013:258, 23 April 2013, Para. 56.
32. Case T322/19, *Aisha Muammer Mohamed El-Qaddafi v Council*, ECLI:EU:T:2021:206, 21 April 2021, Para. 52.
33. *Id.*, Paras 61–62.
34. *Id.*, Paras 71–72.
35. *Id.*, Para. 73.
36. Case C-176/13 P, *Council v Bank Mellat*, EU:C:2016:96, 18 February 2016, Para. 76; Case T-348/13, *Kadhaf Al Dam v Council*, EU:T:2014:806, 24 September 2014, Paras 66–67; Case T-485/15, *Alsharghawi v Council*, EU:T:2016:520, 20 Sept. 2016, Para. 30.
37. Case T322/19, *Aisha Muammer Mohamed El-Qaddafi v Council*, ECLI:EU:T:2021:206, 21 April 2021, Para. 88.
38. Case C-584/10 P, Case C-593/10 P and Case C-595/10 P, *Commission and Others v Kadi*, EU:C:2013:518, 18 July 2013, Paras 119, 121 and 122.
39. Case T322/19, *Aisha Muammer Mohamed El-Qaddafi v Council*, ECLI:EU:T:2021:206, 21 April 2021, Para. 102.
40. *Id.*, Para. 107.
41. *Id.*, Paras 115–117.
42. Case C-599/16, *Oleksandr Viktorovych Yanukovich v Council*, ECLI:EU:C:2017:785, 19 October 2017.
43. Case C-376/10 P, *Tay Za v. Council*, ECLI:EU:C:2012:138, 13 March 2021.
44. Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extraterritorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, as last amended by Commission Delegated Regulation (EU) 2018/1100 of 6 June 2018.
45. Case C-124/20, *Bank Melli Iran, Aktiengesellschaft nach iranischem Recht v Telekom Deutschland GmbH*, Opinion of Advocate General Hogan, 12 May 2021.
46. Formerly known as the Joint Comprehensive Plan Of Action (“JCPOA”), the Iran nuclear deal consists of a political agreement between the five Permanent Members of the UN Security Council, in view of Iran dismantling much of its nuclear program in exchange for the gradual lifting of certain economic sanctions.
47. Executive Order 13846 of 6 August 2018, Reimposing Certain Sanctions With Respect to Iran, entering into effect on 5 November 2018. Bank Melli Iran had previously been listed since 2007, pursuant to Executive Order 13382 of 28 June 2005 – before those sanctions were lifted by the JCPOA.
48. Article paragraph 1 of the EU blocking statute: “no person referred to in Article 11 shall comply, whether directly or through a subsidiary or other intermediary person, actively or by deliberate omission, with any requirement or prohibition, including requests of foreign courts, based on or resulting, directly or indirectly, from the laws specified in the Annex or from actions based thereon or resulting therefrom”.
49. Case C-124/20, Request for a preliminary ruling from the Hanseatisches Oberlandesgericht Hamburg (Germany), *Bank Melli Iran, a public limited company under Iranian law v Telekom Deutschland GmbH*, 5 March 2020.
50. Case C-124/20, *Bank Melli Iran, Aktiengesellschaft nach iranischem Recht v Telekom Deutschland GmbH*, Opinion of Advocate General Hogan, 12 May 2021, Paras 5 and 136–137.
51. *Id.*, Paras 53–65.
52. *Id.*, Paras 66–81.
53. *Id.*, Para. 98.
54. *Id.*, Para. 88.
55. *Id.*, Paras 100–135.
56. Court of The Hague, 25 June 2019, ECLI:NL:RBDHA:2019:6301.
57. Court of The Hague, 25 June 2019, ECLI:NL:RBDHA:2019:6301, Para. 136.
58. Case C-340/20, *Bank Sepah v Overseas Financial Limited, Oaktree Finance Limited*, Opinion of Advocate General Pitruzzella, 17 June 2021.
59. Case C-340/20, Request for a preliminary ruling from the Cour de Cassation (Paris, France), *Bank Sepah v Overseas Financial Limited, Oaktree Finance Limited*, 24 July 2020.
60. Council Regulation (EC) No 423/2007 of 19 April 2007 concerning restrictive measures against Iran and Council Regulation (EU) No 961/2010 of 25 October 2010 on restrictive measures against Iran and repealing Regulation (EC) No 423/2007.
61. Earmarking effect is to be understood as no direct withdrawal effect.

62. Case C-340/20, *Bank Sepah v Overseas Financial Limited, Oaktree Finance Limited*, Opinion of Advocate General Pitruzzella, 17 June 2021, Para. 32.
63. *Id.*, Para. 63.
64. European Parliament, 'An EU human rights sanctions regime?', *European Parliamentary Research Service* April 2019; Eckes, 'The Law and Practice of EU Sanctions', S. Blockmans, & P. Koutrakos (Eds.), *Research Handbook on the EU's Common Foreign and Security Policy*, 2018, p. 23.
65. Case C 46/19 P, *Council v Kurdistan Workers' Party (PKK)*, ECLI:EU:C:2021:316, 22 April 2021.
66. C. Eckes, 'The Law and Practice of EU Sanctions', S. Blockmans, & P. Koutrakos (Eds.), *Research Handbook on the EU's Common Foreign and Security Policy*, 2018, p. 24.
67. Case T 303/19, *Viktor Fedorovych Yanukovych v Council*, ECLI:EU:T:2021:334, 9 June 2021.
68. Case T-580/19, *Sayed Shamsuddin Borborudi v Council*, ECLI:EU:T:2021:330, 9 June 2021.



Sebastiaan Bennink is specialised in economic sanctions and export controls. Sebastiaan's practice focuses on all aspects of international trade law and related issues, such as money laundering, terrorist financing, fraud, bribery and corruption, and other compliance-related topics. Sebastiaan regularly represents clients subject to investigation and enforcement proceedings.

Clients highly regard Sebastiaans, direct, clear and practical advice, as well as his sharp legal analyses, his result-driven approach and in-depth knowledge of their business. Sebastiaan regularly speaks at national and international conferences and gives trainings on sanctions and export controls on a regular basis.

Additionally, Sebastiaan is BNR Newsradio's expert on sanctions and export controls and is often interviewed on the radio and on Dutch national television. Sebastiaan is also regularly quoted in the newspapers (FD and Trouw) on sanctions and export control matters.

BenninkAmar Advocaten
Amstelveenseweg 500
1081 KL Amsterdam
The Netherlands

Tel: +31 6 1268 6437
Email: sebastiaan.bennink@batradelaw.com
URL: www.batradelaw.com



Shanne Verkerk represents companies and individuals charged with financial offences such as fraud, bribery, money laundering and violations of sanctions and export controls. She has extensive experience in both criminal and administrative enforcement proceedings and is dedicated to assisting her clients, if necessary in court.

Prior to joining BenninkAmar, Shanne was a lawyer at Stibbe. She has also acquired knowledge in the field of criminal law through years of work as a legal associate at the criminal court. In this capacity, she provided training on digitalisation within the Dutch courts.

Shanne obtained her Master's of Law (criminal law and criminal procedural law) and her Master's of Science (security policy and law enforcement) at the University of Leiden. She studied international criminal law and human rights at Monash University in Melbourne. She follows closely the developments in Business & Human Rights and enjoys publishing articles in her field of work. She is a member of the Dutch Association of Young Criminal Defence Lawyers.

BenninkAmar Advocaten
Amstelveenseweg 500
1081 KL Amsterdam
The Netherlands

Tel: +31 6 1170 2269
Email: shanne.verkerk@batradelaw.com
URL: www.batradelaw.com



Sarah Reilly is specialised in white-collar defence, regulatory and compliance, and works on cross-border financial and criminal matters. Sarah also assists companies in navigating the regulatory framework of sanctions and export controls and applying for trade licences.

Prior to joining BenninkAmar, Sarah was a lawyer at Navacelle, a boutique firm in Paris. Avocate with the Paris Bar, Sarah advised clients in corruption, money-laundering and insider trading cases and carried out internal investigations in Europe, Asia and Africa. She also conducted compliance monitorships under Negotiated Resolution Agreements with the World Bank.

Sarah acquired a comparative law perspective by graduating with a dual-degree in English and French Law (LL.B., Master 1) from King's College London and Sorbonne, before studying international criminal law at University of Amsterdam and Columbia Law School (LL.M.). Sarah's deep-rooted interest in transitional justice and the rule of law led her to take up traineeships in international organisations and tribunals, namely Human Rights Watch and the Extraordinary Chambers in the Courts of Cambodia.

BenninkAmar Advocaten
Amstelveenseweg 500
1081 KL Amsterdam
The Netherlands

Tel: +31 6 1911 5709
Email: sarah.reilly@batradelaw.com
URL: www.batradelaw.com

BenninkAmar assists its clients in all aspects of sanctions, export controls and other trade law matters. In light of the increase in trade law regulations and enforcement measures globally, BenninkAmar has a proactive approach to trade law in international business and offers tailored advice to its clients, helping them navigate a complex legal landscape, ensure their compliance with applicable trade laws, while enabling them to focus on their business opportunities.

BenninkAmar is the only law firm in the Netherlands that is fully dedicated to sanctions, export controls and trade law matters, and has established an international network of experts and peer law firms. Its client base is diverse and includes numerous publicly listed multinationals, operating in multiple industries and across the US, EMEA, African and Asian regions. BenninkAmar is successful in securing optimal results with supervisory authorities, including OFAC and EU authorities, efficiently resolving

enforcement issues. Its growing team of lawyers contributes to the international trade law community, by being at the forefront of informed interpretive guidance on sanctions, export controls, and all trade law developments.

www.batradelaw.com



**Bennink
Amar**

Australia

Johnson Winter & Slattery



Robert Wyld



Lara Douvartzidis

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Australia implements two types of economic sanctions:

1. United Nations Security Council (**UNSC**) multilateral sanctions, which Australia imposes as a member of the United Nations (**UN**) under the *Charter of the United Nations Act 1945* (Cth) (the **UN Act**); and
2. autonomous sanctions which Australia imposes as part of its independent foreign policy under the *Autonomous Sanctions Act 2011* (Cth) (the **Sanctions Act**) and *Autonomous Sanctions Regulations 2011* (Cth) (the **Sanctions Regulations**). Contraventions of the Sanctions Act and Regulations give rise to serious penalties involving imprisonment and/or significant fines.

Australian sanction laws apply broadly (with potential extra-territorial effect), including in relation to activities:

- in Australia;
- by Australian citizens and Australian-registered bodies corporate overseas; and
- on board Australian-flagged vessels and aircraft.

The type of sanctions imposed use four different measures, depending on the circumstances and objectives of the sanction. These are:

1. restrictions on trade in goods and services;
2. restrictions on engaging in commercial activities;
3. targeted financial sanctions on designated persons and entities; and
4. travel bans on certain persons.

Restrictions on trade in goods and services prohibits the export and import of certain goods and the provision of certain services. Typically, these restrictions prohibit goods and services to a country or region subject to the sanction; however, the restrictions can also be imposed on individuals, entities or groups.

Restrictions on engaging in commercial activities prohibit certain commercial activities (such as purchasing or selling shares) with companies that are operating in nominated industries or providing credit to certain offending entities.

Targeted financial sanctions specifically target certain goods and services to prohibit the supply to designated persons and entities, and prohibit directly or indirectly making an asset available to (or for the benefit of) a designated person or entity. Targeted financial sanctions also prohibit an asset holder using or dealing with an asset that is owned or controlled by a designated entity or person (i.e. 'freezing' the asset).

Travel bans prohibit the designated person(s) from entering or transiting through Australia.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The Department of Foreign Affairs and Trade (**DFAT**) is the primary department that both administers and enforces the sanctions regime in Australia. The Australian Minister responsible for sanctions is the Minister for Foreign Affairs (the **Minister**). Prosecutions are undertaken by the independent Commonwealth Director of Public Prosecutions (**CDPP**) who brings prosecutions for serious Commonwealth criminal offences pursuant to the *Director of Public Prosecutions Act 1988* (Cth). The CDPP commences and continues prosecutions in accordance with the Prosecution Policy of the Commonwealth (**Prosecution Policy**). DFAT also maintains a Consolidated List of all entities and persons subject to sanctions.

The newly created Australian Sanctions Office (**ASO**) is the Australian Government's sanctions regulator. It sits within DFAT's Legal Division in the International Security, Humanitarian and Consular Group. As the sanctions regulator, ASO:

- provides guidance to regulated entities, including government agencies, individuals, business and other organisations on Australian sanctions law;
- processes applications for, and issues, sanctions permits;
- works with individuals, business and other organisations to promote compliance and help prevent breaches of the law;
- works in partnership with other government agencies to monitor compliance with sanctions legislation; and
- supports corrective and enforcement action by law enforcement agencies in cases of suspected non-compliance.

In order to promote compliance with Australian sanctions law and respond to possible breaches, ASO operates within a network of federal partners, including the CDPP, the Department of Defence, the Australian Transaction Reports and Analysis Centre (**AUSTRAC**), the Department of Home Affairs (which administers UNSC travel bans, visa restrictions and violations of the *Customs Act 1901* (Cth)), Defence Export Controls (**DEC**), Australian Border Force, and the Australian Federal Police (**AFP**).

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

As of 1 January 2020, DFAT established the ASO which sits within DFAT's Legal Division in the International Security, Humanitarian and Consular Group.

Prior to 2020, an individual could register as a user of the Online Sanctions Administration System (**OSAS**) to contact DFAT in relation to sanctions permits. However, in 2020, OSAS was replaced by a new online platform (titled 'Pax') in order to improve the process for making enquiries regarding Australian sanctions regimes and applying for sanctions permits. User guides will be available to ease this transition and all existing applications will remain in OSAS until finalised. On 1 October 2020, OSAS went live and is now the operating Australian sanctions portal.

Recent developments in Australia include the following:

- On 1 October 2020, Pax went live. It enables a user to register and create an account, which then allows the user to apply for a Sanctions Permit or request an Indicative Assessment. The platform allows the user to track the progress of the application and access outcomes. It also enables the user to communicate with the ASO.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The Australian Parliament imposes sanctions through legislation to give effect to UNSC sanctions and autonomous sanctions.

The UN Act, the Sanctions Act and the Sanctions Regulations give specific powers to the Minister to regulate economic sanctions (such as the recent activity referenced under question 1.3 above). The Minister can make decisions, subject to the whole of Commonwealth Government and Cabinet approval, as to the persons and entities who will be sanctioned, and can initiate investigations (through the ASO and the AFP) and issue permits for activities that would otherwise be sanctioned.

DFAT administers all three legislative regimes and their regulations. ASO and DFAT regulate the administrative and enforcement of these sanctions. The Department of Home Affairs specifically implements all visa restrictions relating to travel bans that are part of Australian sanctions law.

The following prohibitions are included under the legislative regime in the UN Act and the Sanctions Act:

- making a 'sanctioned supply' of 'export sanctioned goods';
- making a 'sanctioned import' of 'import sanctioned goods';
- providing a 'sanctioned service';
- engaging in a 'sanctioned commercial activity';
- dealing with a 'designated person or entity';
- using or dealing with a 'controlled asset'; or
- the entry into or transit through Australia of a 'designated person' or a 'declared person'.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Australia imposes UN sanctions where they are implemented by the UNSC. Once a UN sanction is imposed, it is then up to the Australian Government to implement that sanction through the UN Act, and relevantly for travel plans, the *Migration (United Nations Security Resolutions) Regulations 2007* (Cth).

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

There is no regional body that issues sanctions. Sanctions only apply in Australia by reason of domestic Australian law.

Nonetheless, Australia has been a member of the Financial Action Task Force (**FATF**) since 1990. FATF sets international standards aimed to prevent global money laundering and terrorist financing. FATF issues FATF Recommendations, or FATF Standards, and involves member countries in mutual evaluations, of which Australia last took part in 2015. Money laundering is a common reason for sanctions to be imposed, particularly against designated persons. Due to Australia's positive response and progress in strengthening its framework to tackle money laundering and terrorist financing, FATF re-rated Australia on seven of the 40 existing FATF Recommendations. However, there has been ongoing criticism of Australia's overall anti-money laundering regime, with the Organisation for Economic Co-operation & Development stating, in its Phase 4 Review of Australia, that more needed to be done to address money laundering risks in the real estate sector from the flow of illicit funds into Australia. Sanctions is one tool to address the illicit flow of money.

Australia implements targeted financial sanctions under UNSCR 1718 and its successor resolutions (**Resolutions**). Designations under these Resolutions have automatic legal effect under Australian law. The Minister may also designate the Democratic People's Republic of Korea (**DPRK**) individuals or entities. Following the adoption of UNSC Resolution 2231, Australia introduced the *Charter of the United Nations (Sanctions – Iran) Regulations 2016* (Cth) which provide for designations under UNSC Resolution 2231 to be automatically incorporated under Australian law.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Australia maintains a Consolidated List for the persons and entities that are currently sanctioned by the UNSC and/or autonomously sanctioned. The Consolidated List contains all persons and entities sanctioned including Australian citizens, foreign nationals, and residents in Australia and overseas.

ASO maintains the Consolidated List and updates it regularly to ensure it is up to date with UNSC sanctions.

In addition, under section 15 of the UN Act, the Minister has the power to list, by notice in the Commonwealth Government Gazette, persons and entities upon being satisfied on reasonable grounds that they are:

- a. a person who commits, or attempts to commit, terrorist acts or participates in or facilitates the commission of terrorist acts;
- b. an entity owned or controlled directly or indirectly by such persons; or
- c. a person or an entity acting on behalf of, or at the direction of such persons and entities.

Once an entity is listed pursuant to section 15 of the UN Act, any person holding an asset that is owned or controlled by a listed person or entity (a **frozen asset**) commits an offence if they, without the authorisation of the Minister, use or deal with a frozen asset, or allow it to be used or dealt with, or facilitates the

use of or dealing with it. In addition, any person who, directly or indirectly, makes a frozen asset available to a listed person or entity, without the authorisation of the Minister, commits an offence.

The person or entity that was listed may write to DFAT to request a statement of reasons for the listing. Further, a listed person or entity, or their authorised representative, may make a written submission to the Minister for the purpose of further informing the Ministerial decision as to whether to declare that the listing will continue to have effect.

Should the listed person or entity wish for their name to be removed from the Consolidated List, they may write to the Minister at any time, outlining this request and setting out the circumstances relied upon to justify the application for revocation of a listing.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

There are mechanisms for challenging an addition to the sanctions list depending on what type of list the individual or entity is designated under. The statutory process for being de-listed is as follows:

- a UNSC Listing must be applied for through the UNSC Focal Point for De-listing, through the country of citizenship or residence;
- a UNSC Listing (related to ISIL/Da'esh and Al Qaida) must be applied for through the UN Office of the Ombudsman or through the country or residence; and
- a counter-terrorism (UNSCR 1373) sanctions regime and Australian autonomous sanctions must be applied for through DFAT.

With regard to the Australian autonomous sanctions regime, DFAT directs that requests for de-listing should be made through the Sanctions Contact Page (<https://www.dfat.gov.au/international-relations/security/sanctions/Pages/contacts-and-links>).

Additionally, if an individual believes that an asset, directly or indirectly owned or controlled by that individual, has been frozen in error, that person should contact the asset holder in the first instance. If, following contact with the asset holder, the belief continues that the asset has been frozen in error, an email should be sent to ASO at asset.freezing@dfat.gov.au and the following information should be provided:

- full name and contact details;
- the details of the asset and asset holder, including details of legal or other interest in the asset;
- details of any contact with the asset holder; and
- the reasons for the belief that the asset has been frozen in error.

In relation to the decision to designate or declare a person under the autonomous sanctions regime, the Minister's decision is subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and under common law. This is the one safeguard available under domestic law; however, there is current debate within Australia as to whether judicial review merely secures the minimum requirement that the Minister act in accordance with the legislation, rather than anything more. For example, in recent times, the Commonwealth Australian Parliamentary Joint Committee on Human Rights was of the opinion that judicial review will generally be insufficient, in and of itself, for human rights purposes, especially in relation to the right to a fair hearing.

2.6 How does the public access those lists?

The public can access the Consolidated List through the DFAT's website (<https://www.dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list>) (linking to the current Consolidated List. This will change when it is updated – see current list as at 5 July 2021: https://www.dfat.gov.au/sites/default/files/regulation8_consolidated_24062021.xls).

The public can also subscribe to the ASO's email database to receive emails when the Consolidated List is updated, or subscribe to Commonwealth Gazettal notices, which will include, from time to time, an update to the Consolidated List.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Australia maintains comprehensive sanctions on several countries and regions. The comprehensive sanctions are implemented under the UN Act, Australia's autonomous sanctions and under both systems.

Australia has currently implemented comprehensive sanctions from the UNSC on countries including: Central African Republic; Democratic Republic of the Congo; Guinea-Bissau; Iraq; Lebanon; Mali; Somalia; South Sudan; Sudan; and Yemen. Australia also implements UNSC sanctions against Counter Terrorism (UNSCR 1373), ISIL (Da'esh), the Taliban, and Al-Qaida.

Australia has currently implemented comprehensive sanctions autonomously and through the UNSC on countries including: DPRK; Iran; Libya; and Syria.

Separate to the UNSC, Australia has also currently implemented autonomous sanctions against countries including: Myanmar; Russia; The Former Federal Republic of Yugoslavia; Ukraine; and Zimbabwe.

The DFAT website has further detailed information of each of the sanctions here: <https://www.dfat.gov.au/international-relations/security/sanctions/Pages/sanctions-regimes>.

2.8 Does your jurisdiction maintain any other sanctions?

Yes. Australia maintains sanctions on individuals and entities.

2.9 What is the process for lifting sanctions?

In addition to the process listed under questions 2.4 and 2.5 above, the Australian Parliament also retains the ability to remove sanctions where the sanction itself was imposed by law.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Australia has a complex export control regime that dictates the prohibitions, restrictions and documentation required for importing and exporting products to and from Australia.

The export regime is regulated by the Department of Home Affairs, Department of Agricultural and Water Resources and the Australian Trade and Investment Commission. Other departments can also be involved where the products are related to that department (for example, the export of wine and grape products necessitate that the Australian Wine and Grape Authority will become involved).

There are further regimes for specific exports that relate to military and dual-use goods and technologies. In addition, Australia has a prescriptive permit regime under the *Customs Act 1901* (Cth), which affects the export regime for certain countries and pursuant to certain multilateral trade treaties. In particular, section 50 provides for a prohibition of goods imported into Australia, while section 112 generally prohibits the exportation of goods unless specified conditions or restrictions are complied with.

The Australia Group is an informal multi-State arrangement which aims to allow exporting or trans-shipping countries to minimise the risk of assisting chemical and biological weapon (CBW) proliferation. The Group meets annually to discuss ways of increasing the effectiveness of participating countries' national export licensing measures to prevent would-be proliferators from obtaining materials for CBW programmes.

Participants in the Australia Group do not undertake any legally binding obligations: the effectiveness of their cooperation depends solely on a shared commitment to CBW non-proliferation goals and the strength of their respective national measures.

All states participating in the Australia Group are parties to the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC), and strongly support efforts under those Conventions to rid the world of CBW.

The Australia Group implements Control Lists covering the following:

- Chemical Weapons Precursors.
- Dual-use chemical manufacturing facilities and equipment and related technology and software.
- Dual-use biological equipment and related technology and software.
- Human and Animal Pathogens and Toxins.
- Plant pathogens.

Details of the Australia Group are at <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html>.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

No. Australia has not introduced blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

Australia does not have secondary sanctions in a form similar to the United States. Australia's sanctions must have a territorial jurisdiction which involves an Australian citizen and/or Australian registered entities. The sanctions still apply to Australian citizens and Australian registered entities regardless of the jurisdiction they are operating within, given the laws have an extra-territorial effect. However, the laws create primary offences of contravening sanctions. There is no secondary sanction regime in Australia. If there is any secondary liability, it arises under traditional common law principles and the statutory regime for accessorial liability under the *Criminal Code 1995* (Cth) (**Criminal Code**) (including under 11.1 to 11.5).

Sanctions will apply to persons and entities that are not citizens or incorporated in Australia where their conduct occurs in Australia and/or on Australian vessels/aircraft.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

As noted above, the sanctions are imposed both on countries, organisations (such as ISIL (Da'esh)) and individuals.

However, the sanctions must be complied with by all citizens of, and entities incorporated in, Australia. As a result, the sanctions apply to all activities in Australia and to activities undertaken overseas by Australian citizens and entities incorporated in Australia, and Australian-registered bodies corporate overseas.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

The Australian Government can seek to freeze the assets of a party that is alleged to hold assets or who may deal with an asset that is owned or controlled by a designated person or entity. In addition, the Minister may 'freeze' certain funds or other assets, the consequence of which is that persons and entities are prohibited from dealing with it, as doing so would constitute an offence. This is action taken by the Australian Government, not, traditionally, private litigants.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

The Minister can authorise a sanctions permit to allow a prohibited activity to be undertaken. The permit may have conditions imposed by the Minister. The criteria to obtain a permit depend on which regime (i.e. which country or party) the permit is for. Where the permit is for a sanction that is endorsed by the UNSC, Australia will need to notify and receive approval from the UNSC before a permit is issued.

The application for a permit will require detailed information about the goods and/or services to be provided, the end use of the goods and/or services, the end user and any other relevant parties, and the intended transport for goods and/or services. An individual or entity wanting to submit a sanctions permit may do so by registering as a user of the OSAS.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

DFAT may exercise its discretion to issue a notice requiring a person to give information or documents, including under oath, for the purpose of determining whether a sanction law has been or is being complied with.

In addition to the above, it is an offence under Australian law to provide false or misleading information in connection with the administration of a sanction law. Penalties range from imprisonment for up to 10 years, as well as significant monetary fines. Should a sanctions permit have been granted on the basis of false or misleading information, penalties can be sought by criminal proceedings (see question 4.12 below).

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

There is no explicit reporting requirement for a sanctions compliance programme for entities. However, DFAT arranges and provides free presentations twice a year on Australian sanctions laws for Australian businesses, universities and individuals in major Australian cities (but only if requested to do so).

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes. It is a serious criminal offence of strict liability for breaching an economic sanction or condition on a permit.

Under the Sanctions Act, the offences in sections 16 and 17 are as follows:

- engaging in conduct that contravenes a sanctions law;
- engaging in conduct that contravenes a condition of an authorisation under a sanction law;
- giving false or misleading information or a document to a Commonwealth entity in connection with the administration of a sanction law; and
- giving false or misleading information or a document to another person recklessly as to whether that person, or another, will give it to a Commonwealth entity in connection with the administration of a sanction law.

Under the UN Act, the offences in sections 28 and 29 are expressed in similar terms, with a reference to a 'sanction law' replaced with 'UN sanction enforcement law'.

The maximum penalty for breaching an economic sanction under the Sanctions Act is, per offence, from 1 July 2020, as follows:

- For an individual:
 - ten years' imprisonment; and/or
 - a fine of up to 2,500 penalty units (a penalty unit from 1 July 2020 is AU\$222.00) (presently AU\$555,000).
- For a company:
 - ten thousand penalty units (AU\$2,220,000); or
 - three times the value of the transaction(s) which the court can determine (whichever is the greater).

The penalties under the UN Act are the same as under the Sanctions Act.

The imposition of any penalty following a prosecution and conviction (or a guilty plea) is at the discretion of the sentencing court applying general sentencing principles for Commonwealth offences under the *Crimes Act 1901* (Cth).

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

DFAT and ASO are responsible for investigating criminal economic sanction offences in conjunction with other authorities. ASO has the power to issue a notice to require a person or entities to give information or documents, including sworn evidence. The ASO can then use this information for determining whether a sanction has been complied with. When DFAT and ASO conclude that an offence has been or may have been committed, they will refer the matter to the AFP for further investigation and to the CDPP for prosecution.

4.3 Is there both corporate and personal criminal liability?

Yes, both corporations and individual persons can be held criminally liable for an offence under the Criminal Code and be penalised.

The Criminal Code sets out a statutory regime for the attribution of knowledge of individual officers to a corporation. Under the Criminal Code, physical elements are attributed to a company in circumstances where an employee, agent or officer of a company commits the physical element when acting within the actual or apparent scope of his or her employment or authority. Fault elements are attributed to a company that expressly, tacitly or impliedly authorised or permitted the commission of the offence. The corporation may be found guilty of any offence, including one punishable by imprisonment.

The terms of corporate criminal responsibility are contained in sections 12.1 to 12.6 of the Criminal Code. In summary, these provisions:

- set out important definitions of 'board of directors', 'corporate culture' and 'high managerial agent';
- establish criminal liability on a corporation by attributing the knowledge and conduct of a person to the corporation;
- attribute negligence to a corporation by reference to the corporation's conduct as a whole;
- provide a mistake-of-fact defence of limited application; and
- establish criminal liability for a bad corporate culture (one that condones or tolerates breaches of the law).

A corporation has an available defence to the question of whether any relevant knowledge or intention possessed by a high managerial agent (as opposed to the board of directors) is to be imputed to it, if the corporation had itself exercised due diligence to prevent the conduct occurring that constituted the offence.

This statutory regime is subject to review by the Australian Law Reform Commission, which presented a report to the Australian Government in April 2020. The report has yet to be released.

Further, individuals may be liable as a director or officer of a corporation if conduct in contravention of the UN Act and the Sanctions Act can properly be characterised as conduct in breach of common law and/or statutory director/officer duties (under the *Corporations Act 2001* (Cth)).

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

See question 4.1 above.

The penalties are expressed as a maximum per offence. Any sentence passed by a sentencing court will apply the sentencing process set out in the *Crimes Act 1901* (Cth) and depend upon the facts of each case and the circumstances of the convicted person.

4.5 Are there other potential consequences from a criminal law perspective?

A breach of laws relating to sanctions may also open up an individual or entity to offences under customs and migrations law, as well as fraud, supporting terrorism or trafficking offences, anti-money laundering offences or other crimes set out in the Criminal Code.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

At the time of writing, no civil penalties exist except for sanction offences.

Where companies provide false or misleading information, liability may arise under the Criminal Code for general criminal offences against the Commonwealth, under the *Corporations Act 2001* (Cth) for a breach of directors' duties and under the Australian Consumer Law for misleading or deceptive conduct offences. In addition, if the conduct is sufficiently egregious and impacts the share value of a company, or otherwise causes significant loss to numerous claimants, a class action (under the terms of the Commonwealth class action regime, pursuant to the *Federal Court of Australia Act 1976* (Cth) or State equivalents) may be available to aggrieved victims.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

See questions 1.2 and 4.2 above.

4.8 Is there both corporate and personal civil liability?

Yes, see question 4.3 above.

Under the *Corporations Act 2001* (Cth), the corporate veil of a company may be pierced in some limited circumstances to allow for liability of directors and/or managers in their individual capacity.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

See questions 4.1 and 4.4 above.

4.10 Are there other potential consequences from a civil law perspective?

Depending upon the conduct, the general fraud, financial deception and dishonesty offences in the Criminal Code may apply. Other civil offences, aside from director/officer duty principles, are limited.

There is an increasing emphasis of Corporate Social Responsibility within the corporate sphere in Australia. For example, shareholders are holding companies to account at an increased rate and demanding transparency in a world increasingly influenced by global investigative reporting. It remains to be seen the extent to which these issues translate into a duty recognised by Australian law as forming part of the duties a director and officer owe to a company, for example, not to engage in conduct in breach of sanctions law which is not in the exercise of power or discharge of a duty with the degree of care and diligence that a reasonable person would exercise in such a position (see section 180(1) of the *Corporations Act 2001* (Cth)).

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

The enforcement of sanctions in Australia is criminal, not civil.

The Australian Government agencies involved in the enforcement of sanctions are DFAT, the AFP and the CDPP. In general terms, the AFP and DFAT will investigate and the CDPP will prosecute. All criminal trials are public unless circumstances exist to justify suppression or non-publication orders. There is generally less publicity until an open trial where admissible evidence is made public. The CDPP does not comment on any existing investigations or prosecutions before the courts. All sentences are public unless there is a good reason (for example, other co-accused are still to stand trial) to make judgments and sentences subject to non-publication orders.

If there are judicial review proceedings, challenging the determination of the Minister or of DFAT, these are civil administrative appeal proceedings in the Federal Court of Australia. They are conducted in accordance with the requirements of the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and the rules of the Federal Court of Australia. Again, these are public unless court non-publication orders are justified.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Any appeal of a criminal conviction for a sanctions offence must be lodged within a specified time, and involves an appeal against conviction and/or sentence. Appeals are to the Court of Appeal in each State where an original trial was held in a State court (exercising Commonwealth jurisdiction) or the Federal Court of Australia. Most criminal proceedings are conducted in State courts, which are entitled to exercise Commonwealth jurisdiction in respect to conduct occurring in a particular State. Appeal proceedings are governed by the relevant Rules of Court applicable to the State or Federal Court.

There have been two publicised proceedings for contraventions of economic sanctions, as outlined below:

- Between March 2009 and April 2010, two individuals were alleged to have exported 90 tonnes of nickel alloys to Iran. Nickel is a banned export to Iran as its potential end use could contribute to Iran's nuclear programme. The nickel alloys were purchased by a Dubai-based company that effected an indirect transfer of the goods to Iran. The AFP launched an investigation in 2012 over allegations 90 tonnes of the banned material was sent to Iran in two shipments falsely labelled as stainless steel.
- One individual pleaded not guilty and proceeded to trial. The matter is ongoing and currently subject to non-publication orders.
- Another individual pleaded guilty in May 2019 on two counts of conduct in contravention of the UN Act and of giving false information to another person, reckless in that it would be given to the Commonwealth in connection with the administration of the sanctions regime in contravention of the UN Act. On 24 December 2019, that person was sentenced to an Intensive Corrections order (18 hours of community service per month for two years) by the District Court of New South Wales.
- In *R v Chan Han Choi*, one individual was charged with breaching UN sanctions for the supply of products related to the proliferation of weapons of mass destruction to the DPRK. The AFP's Operation Byahaut investigated and arrested an individual who was acting as an economic agent of DPRK. It was alleged that Mr. Choi was brokering the sale of missiles and missile componentry and expertise from DPRK to other international entities; and attempting to transfer coal from DPRK to entities

in Indonesia and Vietnam. Mr. Choi was charged with offences under s 27(1) of the UN Act, Regulation, 11(2) of the *Charter of the United Nations (Sanctions – Democratic People’s Republic of Korea) Regulations 2008* (Cth), s 11 of the *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995* (Cth), s 16(1) of the *Sanctions Act and Regulation* and 13(1) of the *Autonomous Sanctions Regulations 2011* (Cth). The trial was listed before the Supreme Court of New South Wales in February 2021, however on the eve of the trial, Mr. Choi pleaded guilty to one count of contravening a United Nations sanction enforcement law and another of contravening a Federal sanction law. The remaining five charges were withdrawn. On 23 July 2021, the NSW Supreme Court sentenced Mr. Choi to three years and six months’ imprisonment for brokering the sale of missile parts, as well as coal and other commodities, in contravention of Australian and United Nations sanctions. As Mr. Choi had been in custody prior to trial for more than the sentence, he walked free from court after being sentenced. The sentencing judgment is *R v Choi* [2021] NSWSC 891, available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NWSC/2021/891.html?context=1;query=choi;mask_path=au/cases/nsw/NWSC.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Australia’s sanctions offences give rise to criminal offences under the Criminal Code and are enforced at a national level. Offending conduct is investigated by the AFP. Prosecutions are conducted by the CDPP.

In relation to investigations, the AFP cooperates within each State and Territory locally and may draw upon and conduct joint taskforces with State and Territory enforcement agencies when conducting investigations, as the circumstances may require it.

4.14 What is the statute of limitations for economic sanctions violations?

There are no statutes of limitation for contraventions of economic sanctions as a serious criminal offence.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

The following legislation is not specifically regarded as economic sanctions, but are nonetheless related to the topic, including:

- *Weapons of Mass Destruction (Prevention of Proliferation) Act 1995* (Cth): <https://www.legislation.gov.au/Details/C2018C00445>.
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth): <https://www.legislation.gov.au/Details/C2019C00011>.
- *Criminal Code 1995* (Cth): <https://www.legislation.gov.au/Details/C2020C00245>.
- *Foreign Acquisitions and Takeovers Act 1975* (Cth): <https://www.legislation.gov.au/Details/C2020C00023>.
- *Foreign Influence Transparency Scheme Act 2018* (Cth): <https://www.legislation.gov.au/Details/C2019C00133>.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Guidance

- DFAT website ‘Australia and sanctions’: <https://www.dfat.gov.au/international-relations/security/sanctions/Pages/sanctions-regimes>.
- Central African Republic and Democratic Republic of the Congo sanctions regimes: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/central-african-republic-and-democratic-republic-congo-sanctions-regimes-sanctions-regime>.
- Counter-Terrorism (UNSC 1373) sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/counter-terrorism-uns-1373-sanctions-regime>.
- Crimea and Sevastopol sanctions regimes: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/crimea-and-sevastopol-sanctions-regime>.
- Democratic People’s Republic of Korea (North Korea) sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/democratic-peoples-republic-korea-sanctions-regime>.
- Former Federal Republic of Yugoslavia sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/former-federal-republic-yugoslavia-sanctions-regime>.
- Guinea-Bissau sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/guinea-bissau-sanctions-regime>.
- Iran sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/iran-sanctions-regime>.
- Iraq sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/iraq-sanctions-regime>.
- ISIL (Da’esh) and Al-Qaida sanctions regimes: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/isil-daesh-and-al-qaida-sanctions-regime>.
- Lebanon sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/lebanon-sanctions-regime>.
- Libya sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/libya-sanctions-regime>.
- Mali sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/mali-sanctions-regime>.
- Myanmar sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/myanmar.aspx>.
- Russia sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/russia.aspx>.
- Somalia sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/somalia.aspx>.
- Sudan and South Sudan sanctions regimes: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/sudan-and-south-sudan-sanctions-regime>.
- Syria sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/syria.aspx>.

- The Taliban sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/the-taliban.aspx>.
- Ukraine sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/ukraine.aspx>.
- Yemen sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/yemen.aspx>.
- Zimbabwe sanctions regime: <https://www.dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/zimbabwe.aspx>.

Legislation

- *Charter of the United Nations Act 1945* (Cth) – regulations: <https://www.legislation.gov.au/Details/C2016C00742>.
- *Autonomous Sanctions Act 2011* (Cth) – regulations: <https://www.legislation.gov.au/Details/C2016C00247>.
- *Weapons of Mass Destruction (Prevention of Proliferation Act 1995)* (Cth): <https://www.legislation.gov.au/Details/C2018C00445>.
- *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth): <https://www.legislation.gov.au/Details/C2019C00011>.
- *Criminal Code 1995* (Cth): <https://www.legislation.gov.au/Details/C2020C00245>.
- *Foreign Acquisitions and Takeovers Act 1975* (Cth): <https://www.legislation.gov.au/Details/C2020C00023>.
- *Foreign Influence Transparency Scheme Act 2018* (Cth): <https://www.legislation.gov.au/Details/C2019C00133>.
- Consolidated List: <https://www.dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list>.



Robert Wyld is one of Australia's leading commercial crime lawyers. For over 30 years, he has practised in commercial crime, including fraud, bribery, corruption, money laundering, sanctions, extradition and internal corporate investigations. He has represented individuals and leading companies in relation to internal and external investigations and prosecutions. Robert has advised various clients on Australia's sanctions regime and on the United States sanctions regime in a variety of industries and sectors.

He has published extensively in Australia, the United Kingdom, Germany and the United States (with Oxford University Press). Robert has been recognised as a leading Business Crime, Investigations & Asset Recovery lawyer by *Who's Who Legal* Australia 2017 to 2021 inclusive, is the only *Who's Who* Thought Leader in Investigations for Australia and is regularly ranked as a Band 1 *Chambers Asia Pacific* lawyer for bribery and anti-corruption work.

Johnson Winter & Slattery
Level 25, 20 Bond Street
Sydney, NSW 2000
Australia

Tel: +61 2 8274 9593
Email: robert.wyld@jws.com.au
URL: www.jws.com.au



Lara Douvartzidis is a rising talent at Johnson Winter & Slattery, one of Australia's leading independent law firms. As an associate, Lara works with partners across the firm to advise major Australian and international corporations on their most challenging legal issues, with a focus on *pro bono* and commercial litigation, environment and planning law, class actions, and modern slavery law obligations. Lara assists in expanding the firm's *pro bono* practice as a *pro bono* coordinator. She is passionate about strategic litigation trends, including the convergence of international human rights law with national and international environmental law.

Lara previously served as the Associate to the Honourable Chief Justice Kourakis of the Supreme Court of South Australia. She has been recognised in *Australasian Lawyer's* 2021 Rising Stars list. She holds an Advanced Master's in European and International Human Rights Law from Leiden University in The Hague and is a valued member of the Business and Human Rights Subcommittee for the Australian Lawyers for Human Rights.

Johnson Winter & Slattery
Level 25, 20 Bond Street
Sydney, NSW 2000
Australia

Tel: +61 2 8247 9657
Email: lara.douvartzidis@jws.com.au
URL: www.jws.com.au

Johnson Winter & Slattery is one of Australia's leading independent law firms, and is regularly engaged by major businesses, investment funds and government agencies as legal counsel on important transactions and disputes throughout Australia and surrounding regions. We are a full-service commercial firm with specialist expertise in all facets of commercial activity, covering the spectrum of transactional needs, advisory, compliance and investigations, as well as dispute resolution.

We help our clients navigate legal complexity by applying specialist legal expertise, innovative technology and commercial awareness to our clients' business objectives. Commitments to outstanding client service, a collaborative ethos and the importance of fashioning commercial outcomes are hallmarks of our firm.

www.jws.com.au

JOHNSON WINTER & SLATTERY

Austria

Dorda Rechtsanwälte GmbH



Bernhard Müller



Heinrich Kühnert

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

The Austrian sanctions regime is almost exclusively based on sanctions measures adopted by the United Nations (“UN”) and the European Union (“EU”). The Austrian Sanctions Act (*Sanktionengesetz* – “SanktG”) essentially regulates the domestic implementation of these sanctions. Only if the UN Security Council were to adopt resolutions concerning terrorist groups in Europe would these UN sanctions have to be implemented in national law as the EU does not currently have the power to regulate such matters.

Pursuant to Sec 2 of the SanktG, the Austrian National Bank (*Österreichische Nationalbank* – “OeNB”) is responsible for national implementing measures, in particular, regarding the freezing of assets. The Austrian Federal Government (*Bundesregierung*), on the other hand, is responsible for:

- the confiscation of means of transport and goods;
- prohibiting the provision of services; and
- the exemption from the obligation to comply with civil claims relating to contracts or other legal transactions affected by sanctions of the UN or the EU, etc.

National implementation measures are to be issued either in the legal form of a regulation (*Verordnung*) or an administrative decision (*Bescheid*).

The enactment and revocation of the OeNB's regulations require the consent of the Federal Government; in the event of imminent danger, the consent of the Federal Chancellor (*Bundeskanzler*) is sufficient. The enactment of regulations by the Federal Government requires the consent of the main committee (*Hauptausschuss*) of the National Council (*Nationalrat* – Nationalrat is one of the two chambers of the Austrian Parliament; the other chamber is the representation of the nine provinces [*Bundesrat*]; and the *Hauptausschuss* is a parliamentary organ of Nationalrat which participates in the administration at the federal level [*Bund*]).

In addition to the sanctions regime, Austria also has an export control regime. For further details, see question 2.10.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The responsibilities of the Federal Government and the OeNB with regard to domestic implementing measures have already been mentioned in question 1.1 above. In addition, the following competencies regarding sanctions exist:

In Austria, the Ministry for Europe, Integration and Foreign Affairs (*Bundesministerium für Europa, Integration und Äußeres*) is

responsible for dealing with and coordinating international sanctions (in particular, within the framework of the UN and the EU and for legal issues in connection with the negotiation and implementation of sanctions).

The Federal Minister of the Interior (*Bundesminister für Inneres*) plays an important role here and is responsible for monitoring the domestic implementation of sanctions, except for legal acts pursuant to Sec 2 SanktG enacted by the OeNB (see question 1.1 above).

In addition, the land register courts (*Grundbuchsgerichte*) and commercial register courts (*Firmenbuchsgerichte*) have certain functions in connection with the recording in the land register (*Grundbuch*) or commercial register (*Firmenbuch*) that certain assets are frozen. With regard to assets which are frozen on the basis of a legal act of the Federal Government, or on the basis of directly applicable sanction measures of the EU in the land register or the commercial register, the Federal Minister of the Interior shall notify the court competent for the property or the legal entity of this fact. Based on this notification, the court shall *ex officio* enter in the land register or the commercial register that the assets of the person or institution concerned are frozen.

Finally, the individual other federal ministries (*Bundesministerien*) are also obliged under the Federal Ministries Act (*Bundesministerien-gesetz*) to take any implementing measures for the implementation of sanctions in their own sphere of influence.

The Federal Ministry for Digital and Economic Affairs (*Bundesministerium für Digitalisierung und Wirtschaftsstandort*) is the national authority for the enforcement of the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz* – “AußWG”) and the associated implementing regulations.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

No, there has not.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

There are no legal or administrative authorities in Austria that can impose sanctions. As explained above in questions 1.1 and 1.2, in Austria the competent authorities can only adopt national implementing measures under the SanktG. These are primarily the responsibility of OeNB. Further responsibilities lie with

the Federal Government as a collegial body, the Ministry for Europe, Integration and Foreign Affairs and the Ministry of the Interior, as well. Measures under foreign trade law are the responsibility of the Ministry for Digital and Economic Affairs.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes. Concerning the implementation of UN actions, see questions 1.1 and 1.2. We are not aware of any significant failure to implement UN sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

This is not applicable. Austria is, of course, a Member State of the EU and participates in the development of EU sanctions in the relevant bodies. We understand the EU as a supranational organisation, but not as a “regional body” in the sense of this question.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Austria does not keep its own lists of sanctions. However, there are domestic implementation measures pursuant to Sec 2 SanktG, which are issued by regulation or through an administrative decision of the OeNB or the Federal Government. These ordinances also list the persons, groups and organisations concerned.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

It is possible to challenge implementation measures pursuant to Sec 2 SanktG in the form of an ordinance before the Constitutional Court (*Verfassungsgerichtshof*). An appeal may be lodged against administrative decisions of the OeNB or the Federal Government, which shall be decided by the Federal Administrative Court (*Bundesverwaltungsgericht*) at first instance and finally by the Supreme Administrative Court (*Verwaltungsgerichtshof*).

So far, there has been no case law available on this subject in Austria.

2.6 How does the public access those lists?

As set out above, Austria does not keep its own lists of sanctions. However, the ordinances of the OeNB (see question 2.4) are published on its homepage or must be published in the Federal Law Gazette (*Bundesgesetzblatt*).

With regard to entries in the land register (*Grundbuch*) and the commercial register (*Firmenbuch*) (see question 2.1), it should be noted that these are public registers which can be inspected by anyone.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

This is not applicable in Austria.

2.8 Does your jurisdiction maintain any other sanctions?

This is not applicable in Austria.

2.9 What is the process for lifting sanctions?

Since Austria does not have its own sanctions regime, sanctions are lifted at EU or UN level. National implementation measures pursuant to Sec 2 paras 1 and 2 SanktG must be revoked as soon as the underlying sanction measures of the UN or the EU are repealed.

If a domestic legal act is subsequently repealed pursuant to Sec 2 para. 1 or directly applicable sanction measures of the EU, the Federal Minister of the Interior shall inform the competent court that it will delete the entries made in the land register or the commercial register (see question 2.1).

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

In addition to the sanctions regime, which is essentially based on EU and UN sanctions, Austria also has its own export control regime. The legal basis for this is the AußWG. Essential areas of regulation of the AußWG are:

- export control, in particular concerning export, transit, brokerage of defence and dual-use products (accompanying provisions of Regulation (EC) no 428/2009) and the provision of technical assistance for military end-use; and
- control of the movement of defence-related products within the EU for the implementation of Directive 2009/43/EC.

In addition, Austrian law provides for the control of takeovers of Austrian companies by persons or companies from third countries (outside the EU, EEA, Switzerland); approval is only required for the takeover of companies in certain critical sectors. The Investment Control Act extends the scope of the approval requirement for a number of industries, from previously 25 per cent to a 10 per cent voting interest in the target company. Moreover, indirect investments also come within the scope of the Act. The assessment criteria refer to the impact of the takeover on security and public order, including the provision of basic needs and crisis prevention.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

This is regulated on an EU-wide basis by Regulation (EC) no 2271/96 (the “EU Blocking Regulation”). The only law passed by the Austrian legislator in this regard (Federal Gazette No I 117/1997) determines the level of fines for infringements of the EU Blocking Regulation. The maximum fine currently amounts to approx. EUR 73,000.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as “secondary sanctions”)?

No, it does not.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

This is not applicable in Austria.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

The OeNB's implementation measures mainly affect banks, which are responsible for freezing the accounts and credit balances concerned.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

If it does not oppose the purpose of the sanctions, the OeNB may grant specific authorisations, in particular for the use of frozen funds or making assets available for essential human needs, and furthermore for payments of taxes, compulsory insurance premiums and fees for public utility services, such as gas, water, electricity and telecommunications, and payments of claims originating before the adoption of sanction measures. Requests for authorisation shall be made to the OeNB.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

In the exercise of their functions, the Federal Minister of the Interior and the OeNB are entitled to request the necessary information and notifications from natural and legal persons and from other entities possessing legal personality, and to identify and process data; this right also includes the power to consult on-site books, documents and computer data carriers and to duplicate them. If the information or documents provided are insufficient, or if there is reasonable doubt concerning the accuracy or completeness of the information or documents, the Federal Minister of the Interior and the OeNB shall be entitled to request respective explanations or evidence.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

This is not applicable in Austria.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

There exist both administrative penal (*verwaltungsstrafrechtliche*) provisions and criminal penal (*strafrechtliche*) provisions.

Administrative penal fines are imposed by public authorities and not by courts, and are normally lower than criminal penalties, although detention measures are the exception. These criminal and administrative penal provisions are set out in Sec 11 *et seq.* of the SanktG and are generally applicable in case national measures implementing sanctions have been breached. Administrative penal sanctions are similar to those understood as "civil penalties" or "civil fines" in the UK or US.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The prosecution of criminal offences is the responsibility of the public prosecutor's offices (*Staatsanwaltschaften*). The prosecution of administrative offences is the responsibility of the local district administrative authority (*Bezirksverwaltungsbehörde*) or, if available, the *Landespolizeidirektion*.

4.3 Is there both corporate and personal criminal liability?

Criminal penal provisions in Austria are basically only applicable to natural persons. However, some years ago the concept of corporate responsibility for criminal conduct of associations (*Verbände*) was introduced to the Austrian legal system, and is regulated by the Act on Corporate Criminal Liability (*Verbandsverantwortlichkeitsgesetz – "VbVG"*). Pursuant to the VbVG, legal entities can be held responsible and fined for criminal offences which have been committed in favour of the legal entity or are attributable to the legal entity by the misconduct of its management.

As to administrative offences, corporate liability does not exist. In administrative criminal law, the persons appointed to represent the company externally, i.e. the management, are punished. Legal entities, however, are jointly and severally liable for the penalties imposed on management.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

The fines for administrative offences are up to EUR 50,000 per offence. The attempt is also punishable. In the case of a criminal penal provision, the offender is to be punished with a prison sentence of up to one year or a fine of up to 360 daily rates. The amount of the daily rates depends on income.

4.5 Are there other potential consequences from a criminal law perspective?

Persons who carry out certain economic activities or perform certain management functions must be reliable. This applies not only to certain sensitive trades (*sensible Gewerbe*) but also to the managers (*Geschäftsleiter*) of a bank. Persons who have been punished for infringements under the SanktG could therefore lack the reliability to carry out certain occupations: the function of a managing director under trade law (*gewerberechtlicher Geschäftsführer*); or the managing director of a bank. In award procedures under EU and Austrian public procurement law, the reliability of the management of a bidder is also checked, and there could be a risk of exclusion from the award procedure if a member of management was punished for violating sanctions.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

See our answers to questions 4.1 to 4.5. Civil penalties can be compared to “administrative penal sanctions” or “administrative fines” in Austria.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

This is not applicable in Austria.

4.8 Is there both corporate and personal civil liability?

This is not applicable in Austria.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

This is not applicable in Austria.

4.10 Are there other potential consequences from a civil law perspective?

This is not applicable in Austria.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

Decisions of the authority on administrative penalties are not public. Judicial criminal proceedings are open to the public, but first instance judgments are not published. Decisions of administrative courts (*Verwaltungsgerichte* – the administrative penalty imposed by the authority may be challenged before an administrative court) and courts of appeal (*Berufungsgerichte*) (concerning judicial offences) are published anonymously on the internet.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

So far, no case law is available in Austria.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

In Austria, the federal provinces have no regulatory power with regard to sanctions.

4.14 What is the statute of limitations for economic sanctions violations?

For administrative offences, a statutory limitation period of 18 months applies. For criminal offences, a statutory limitation period of three years applies.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

Even if these are not “economic sanctions-related measures” in the narrower sense, the “legal fate” of civil law contracts must be mentioned as a possible negative side effect of sanctions. The Austrian legal system does not contain any explicit provisions in this regard.

- In Austrian civil law (Sec 879 of the Austrian General Civil Code – *Allgemeines Bürgerliches Gesetzbuch* – “ABGB”), however, there is a provision setting out that contracts that violate legal prohibitions are null and void, or at least floating void. However, there is no case law as to whether sanctions are such a “legal prohibition”.
- In addition, one could also consider whether contracts that violate sanctions are impossible within the meaning of Sec 878 ABGB because they may not be fulfilled, and therefore a withdrawal from the contract is possible.
- Furthermore, many contracts contain a *force majeure* clause. The adoption of international sanctions can be qualified as *force majeure*. Therefore, such a *force majeure* clause will give the parties the right of withdrawal from the contract or at least the freedom from performance.
- Finally, in the case of continuing obligations, there is a generally accepted legal principle in Austria that a contracting party can terminate such a continuing obligation for important reasons (i.e., if it becomes unreasonable for a contracting party to continue the contractual relationship).

However, there are a few relevant provisions in the SanktG:

- Sec 2 para. 2 no 6 of the SanktG stipulates that the Federal Government may, by ordinance or administrative decision, order exemption from the obligation to fulfil civil law claims if their fulfilment could impair the effectiveness of UN or EU sanctions. On the contrary, at least with respect to existing contracts, one could argue that contracts are not null and void from the outset according to Sec 879 or impossible according to Sec 878 ABGB, but that it is always important whether their fulfilment endangers the purpose of the sanctions. However, there is no relevant case law in Austria on this subject.
- A further provision which refers to the fulfilment of civil law claims can be found in Sec 5 of the SanktG. Accordingly, in connection with civil law claims pursuant to the aforementioned Sec 2 para. 2 no 6 of the SanktG, it rests with the person asserting the civil claim to submit evidence that the compliance with a contract or other legal transaction was not affected by the sanction.
- Additionally, a person fulfilling a civil claim, although not required to do so pursuant to Sec 2 para. 2 no 6, cannot derive third party claims from it, unless the person complied involuntarily or neither knew nor had to know that the claim was not to be complied with pursuant to Sec 2 para. 2 no 6.
- Similarly to Art 6 of EU Regulation no 881/2002, there exists a similar provision in the SanktG. Damages for the delay of or non-compliance with a contract or other legal transaction cannot be claimed if such delay or non-compliance is based on a negligent lack of knowledge that a person or entity is not affected by a legal act pursuant to Sec 2 of the SanktG.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

The Legal Information System of the Republic of Austria (*Rechtsinformationssystem* – “RIS”), which can be accessed online at <https://www.ris.bka.gv.at>, serves to publish the federal law and the law of the provinces. It also serves to provide information on federal and state law and provides access to EU law, case law, etc.

Some Austrian laws have also been translated into English and can be accessed in the RIS like the SanktG. However, these translated laws are not always up to date – this is also the case with the SanktG. Furthermore, it should be noted that only the German version is the authentic and thus binding version.

One can enquire about current law projects and draft laws, as well as about relevant appraisal procedures on the homepage of the Austrian parliament at <https://www.parlament.gv.at>. Here, you can also find explanatory materials on the laws and the decrees of the National Council (see also question 2.10).

See also question 2.6. The OeNB also publishes interpretations and practical information.



Bernhard Müller has been heading the Practice Group "Public & Regulatory Law" at DORDA since 2010, and advises national and international clients in all areas of public commercial law. His practice focuses on EU law, public procurement, regulatory law, sanctions and foreign trade law. His industrial practice concentrates on Life Science, Energy and Defence & Security. Since 2009, Bernhard Müller has been teaching as an Associate Professor of Public Law at the Faculty of Law of the University of Vienna. He therefore brings to his advice not only his extensive practical experience, but also his academic background.

DORDA Rechtsanwälte GmbH

Universitätsring 10
A-1010 Wien
Austria

Tel: +43 1 533 4795 57
Email: bernhard.mueller@dorda.at
URL: www.dorda.at



Heinrich Kühnert is a partner and heads DORDA's antitrust and regulatory practice group. Heinrich advises domestic and international clients on all aspects of Austrian and European competition law (merger control, antitrust, abuse and state aid). He has broad experience in a large number of industries, including the energy, transport, telecom, media, healthcare, mechanical engineering as well as retail sectors. In addition to his advisory work, Heinrich publishes regularly on competition law topics. Heinrich received his legal education at the Universities of Vienna, Oxford and Fribourg (Switzerland).

DORDA Rechtsanwälte GmbH

Universitätsring 10
A-1010 Wien
Austria

Tel: +43 1 533 4795 35
Email: heinrich.kuehnert@dorda.at
URL: www.dorda.at

DORDA Rechtsanwälte GmbH ranks among the leading law firms in Austria and is currently composed of about 80 lawyers. DORDA advises domestic and international clients in all relevant areas of business law. The Practice Group "Public & Regulatory Law" advises clients on all questions of public commercial law, in particular on public procurement law, regulatory law, sanctions and foreign trade law.

www.dorda.at

D O R D A

China

JunHe LLP



Weiyang (David)
Tang



Juanqi (Jessica)
Cai



Runyu (Roy) Liu



Siyu (Rain)
Wang

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

There are two categories of economic sanctions implemented in China. First, China adopted United Nations (“UN”) sanction-related resolutions. With the permanent seat in the UN Security Council, economic sanctions mandated by the resolutions of the UN Security Council became China’s international obligations. Second, China has enacted a number of laws and regulations in 2020 and 2021 to establish its own sanctions against foreign persons as a countermeasure for certain economic sanctions imposed by other countries, as well as certain rules to block the application of unjustifiable extraterritorial foreign laws and measures.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

Normally, UN sanctions are administered primarily by the Ministry of Foreign Affairs (“MFA”) through administrative notices. The programmes are then enforced by various regulatory authorities such as Ministry of Commerce (“MOFCOM”), the People’s Bank of China (the central bank), China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, the Ministry of Transport, the General Customs of China, and the Ministry of Public Security, in their respective authority.

As to China’s own counter-sanctions measures, the MFA and MOFCOM are the primary authorities for administration and enforcement. Other regulatory authorities will be responsible for implementing the countermeasures, such as assets freezing and entry denial.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

Over the past 12 months, China has developed a number of counter-sanctions measures:

Unreliable Entity List

On September 19, 2020, MOFCOM promulgated the *Provisions on the Unreliable Entity List* (the “UEL Provisions”). The UEL targets foreign entities whose activities are considered to have endangered the national sovereignty, security and development interests of China, or undermined the legitimate rights and interests of Chinese enterprises, other organisations or individuals. By now, MOFCOM has not designated anyone onto the UEL.

Blocking Rules

On January 9, 2021, MOFCOM promulgated the *Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures* (the “Blocking Rules”), which are designed to block the application of certain foreign laws and measures that are determined to have the effect of unjustifiably prohibiting or restricting transactions between Chinese persons with third country persons. Please refer to the answer to question 2.11 for detailed discussion.

Anti-Foreign Sanctions Law

On June 10, 2021, the *Anti-Foreign Sanctions Law of People’s Republic of China* (the “Anti-Foreign Sanctions Law”) was adopted by the Standing Committee of the National People’s Congress (“NPC”) and signed into law by Chairman of the PRC. Please refer to the answer to question 2.1 for detailed discussion.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Before the Anti-Foreign Sanctions Law was enacted, the Foreign Trade Law (2016, as amended) provided general legal basis for imposing sanctions and the National Security Law (2015) has provided legal authority for the State Council to take actions as necessary when there is a national security concern. The National Security Law is also the legal authority for sanctions-related rules and measures such as the UEL Provisions and the Blocking Rules.

Now, the Anti-Foreign Sanctions Law has become the primary authority for the Chinese government to impose its own sanctions. The law primarily targets those foreign individuals/organisations that are considered to be actively pursuing or involved in enacting “discriminatory restrictive measures” against China. Any individuals or organisations that directly or indirectly participate in the formulation, decision-making, or enforcement of the “discriminatory restrictive measures” may be placed on the counter-sanctions list. Related individuals and entities of the listed individuals or organisations may also be subject to countermeasures.

Prior to the Anti-Foreign Sanctions Law which was enacted, the MFA had begun its sanctions on certain individuals and entities. So far, more than 70 individuals and organisations have been sanctioned by the MFA, mainly for interfering in China’s internal affairs, or imposing unilateral sanctions on relevant Chinese entities and individuals. The restrictions to those entities typically include banning the targeted persons and their families from entering China (including Hong Kong and Macao), freezing assets in China, and restricting transactions

with organisations and individuals in China. On July 24, 2021, after the Anti-Foreign Sanctions Law was released, the MFA announced sanctions over seven U.S. persons, directly citing the authority under the Anti-Foreign Sanctions Law.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes, China implements UN sanctions through administrative notices. Generally, the MFA would first initiate a notice to notify various government agencies of relevant UN Security Council resolutions and urge the agencies to implement economic sanctions mandated by the resolutions. Various regulatory authorities, such as the General Customs of China, the People's Bank of China, China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, and the Ministry of Transport, would then issue notices to implement measures in their respective jurisdictions.

With respect to how the specific sanction resolutions would be implemented, practices differ, mostly in two manners.

■ **Implementation without additional domestic rules to UN resolutions**

Under most scenarios, UN sanctions-related resolutions are implemented by issuing administrative notices attaching UN resolutions, without any additional domestic rules for government agencies. For example, on September 18, 2014, the Ministry of Transportation just forwarded Resolution 2174 of the UN Security Council (sanctions against Libya which imposes sanctions on certain entities and persons), without adding additional domestic rules to implement this resolution. The Ministry of Transportation also urges all the relevant departments to take responsible measures and strictly implement the UN resolution.

■ **Implementation with additional domestic rules to UN resolutions**

Another way of implementing UN resolutions is adding relevant government agencies' additional rules/interpretations. This practice is more common in the banking area. The China Banking and Insurance Regulatory Commission issued several notices adding their own additional rules when implementing UN economic sanctions resolutions, such as to urge banks:

- to remain on high alert over their businesses and transactions involving sensitive countries or regions;
- to timely check information on international events relevant to their business operations, including the sanction resolutions of the UN;
- to establish and improve the corresponding management information system, timely enter and update the relevant sanction list, clients in suspicious transactions and other information; and
- to prevent an organisation or individual from using the institution for supporting terrorism, money laundering and other illegal activities.

In some limited cases, China does not implement UN resolutions against certain countries/regions due to the political position of the PRC government. At present, China implements UN sanctions against 11 countries, as well as ISIL and Al-Qaida.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

No, China is not a member of any regional body that issues sanctions.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

China adopts the sanction lists of the UN Security Council. It is also changing its position to establish its own list of sanctioned individuals and entities.

UEL

- China establishes a working mechanism with the involvement of relevant departments of central state organs (the "working mechanism") to be responsible for administering the UEL regime. The working mechanism shall initiate on its own or based on suggestions or reports from relevant parties, investigations into the conduct of a foreign entity in accordance with its functions and powers. During the investigation, the foreign entity may make statements and defences. Based on the results of the investigation, the working mechanism will decide whether to place the foreign entity on the UEL.
- Where the subject foreign entity corrects its actions and takes measures to eliminate the consequences of its conduct within the designated time, the working mechanism may decide to remove it from the UEL. In addition, the subject foreign entity can also apply to be removed from the UEL. The working mechanism will review its situation and make a decision.

As of July 2021, no further details or implementing rules regarding the UEL have been made, and no entities or individuals have been designated to the UEL.

Anti-Foreign Sanctions Law

According to the Anti-Foreign Sanctions Law, the MFA or other relevant departments of the State Council will issue orders announcing the determination, suspension, modification or cancellation of the counter-sanction listing and countermeasures. Currently, the MFA announced the sanctions through its press conference, and has not yet established a list of foreign persons subject to the counter-sanctions.

As the law is just enacted recently, the authorities have not yet issued specific procedures for both adding to and removing from the list.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

As to the UEL programme, during the investigation of such UEL listing process, the entity being investigated can make its own statement and defend itself. If the arguments or mitigation measures are accepted, the investigation can be terminated. If the entity has been listed on the UEL, it can only apply for removal.

As to the sanctions imposed under Anti-Foreign Sanctions Law, the law indicates the listing cannot be challenged, and can only be revoked by the authority on its own decision.

2.6 How does the public access those lists?

The UN sanctions list is available on the UN website.

As to the MOFCOM's UEL sanctions, as of July 2021, no individuals/entities have been added to the list.

For the MFA's sanctions, there is no specific sanction list so far. The sanctions are announced by the MFA through its press conference. The public can search on the MFA's official website for such announcements.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Except for adopting UN sanctions and embargoes, China does not maintain its own comprehensive sanctions or embargoes.

2.8 Does your jurisdiction maintain any other sanctions?

As discussed above, the Chinese government has now established its own counter-sanctions regimes under the Anti-Foreign Sanctions Law and the UEL Provisions.

2.9 What is the process for lifting sanctions?

For UN sanctions and embargoes, the process for lifting sanctions depends on the UN's lifting decision.

As to the Chinese sanction lists, the Chinese government has not published any implementing rules regarding the process for lifting sanctions.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes. The framework for Chinese export controls was established in 2002 and underwent a major revision in 2020 with the enactment of the Export Control Law. The main goals of Chinese export controls are non-proliferation of weapons of massive destruction, anti-terrorism and protection of national security.

Under the new Export Control Law, the controlled items include dual-use items, munitions, nuclear and other items related to the maintenance of national security and interests and implementation of non-proliferation and other international obligations. The controlled items cover commodities, technologies, services, as well as data related to those items. Export, re-export and deemed export of such items are all controlled under the law.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Yes. On January 9, 2021, MOFCOM promulgated the Blocking Rules. The Blocking Rules essentially adopts a two-pronged test: (a) whether foreign laws and measures have unjustified extra-territorial application; and (b) whether such foreign laws and measures unjustifiably prohibits or restricts transactions between Chinese persons with third country persons. Although the Blocking Rules do not specify the foreign laws and measures the application of which is to be blocked, which is subject to the government's absolute discretion, U.S. sanctions programmes that have extra-territorial applications (particularly "secondary sanctions") are likely to be blocked under the Blocking Rules.

Chinese Persons have the obligation to report to MOFCOM when they encounter prohibitions or restrictions by such foreign laws and measures. MOFCOM may issue prohibition orders not to recognise, enforce or observe certain unjustified extra-territorial application of foreign legislation and other measures. Further, Chinese persons shall abide by the prohibition order. They can also apply for exemptions to comply with the foreign laws and measures. Until now, MOFCOM has not issued any prohibition orders. The Blocking Rules also give the suffering parties the rights to file civil lawsuits to seek compensation from the party that complies with such foreign laws and measures.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

China has not imposed any secondary sanctions.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

For criminal liabilities, PRC Criminal Law applies to: 1) all crimes committed within the territory of the PRC; 2) PRC citizens who have committed crimes outside the territory of the PRC; 3) foreigners who are outside PRC territory, and have committed crimes against the PRC or its citizens; and 4) crimes specified in international treaties to which the PRC is a signatory state or with which it is a member and the PRC exercises criminal jurisdiction over such crimes within its treaty obligations. Although it remains arguable whether UN Security Council resolutions should be regarded as international treaties under PRC Criminal Law, we have not seen any precedent in which the PRC has asserted jurisdiction over activities violating UN resolutions where no PRC citizens were involved or violations were not committed in the territory of the PRC.

As to administrative liabilities, the PRC government has broad jurisdiction over PRC persons and activities conducted within the territory of the PRC.

Additionally, under Blocking Rules and the Anti-Foreign Sanctions Law, potential civil litigations may be brought by Chinese persons against Chinese or foreign persons who violate the provisions and cause damages to Chinese persons.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

For an entity/individual listed as a sanctioned entity/individual by a UN resolution, corresponding actions including freezing the assets under bank accounts will be taken by a financial institution or a specific non-financial institution.

As to UEL, while the UEL Provisions do not specify such assets freezing measure, it provides a broad authorisation for the authorities to take any measures as it deems necessary once a foreign person is designated onto the UEL, which theoretically may include assets freezing. As there is no precedent so far and no implementing rules have been promulgated, it is unclear.

As to countersanctions imposed under the Anti-Foreign Sanctions Law, blocking or freezing funds or other property within the Chinese jurisdiction is among the measures that can

be taken by the government. Once it is authorised, and Chinese persons are required to block or freeze assets of those sanctioned persons.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

For the UN sanctions adopted by China, there is no such licence available in China, unless authorised by the UN.

As to the countersanctions imposed under the Anti-Foreign Sanctions Law, the law does not specify the licensing mechanism. Since the government has not published implementing rules, it is not known whether there will be any licence available. The law provides that the authorities may decide to suspend, modify or revoke the sanctions and measures when circumstances are warranted, which suggests that parties might submit applications seeking special licences.

Under the UEL Provisions and the Blocking Rules, Chinese persons can apply for exemptions to conducted activities otherwise prohibited; however, there has been no practice yet.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

There are certain reporting requirements in the banking and financial sector. According to the *Notice of the People's Bank of China on Implementing the Relevant Resolutions of the United Nations Security Council*, upon receipt of the notice from the MFA on the implementation of relevant UN sanction resolutions, financial institutions and specific non-financial institutions shall immediately enter information about individuals and entities included in sanction lists into the relevant business systems and conduct a retrospective review. If any of the listed persons are identified, the financial institutions and specific non-financial institutions shall take corresponding actions immediately and report the relevant information to the People's Bank of China and other relevant authorities.

As to the countersanctions under the Anti-Foreign Sanctions Law, Chinese persons are required to implement the countermeasures as announced (such as assets freezing). The law does not specify the reporting procedures for such persons implementing the assets freezing.

As to the Blocking Rules, Chinese persons have the obligation to report to MOFCOM when they encounter prohibitions or restrictions by such foreign laws and measures; however, detailed procedure is unspecified.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

The Chinese government has published a number of compliance guidelines to urge and encourage enterprises to establish compliance programmes. For example, the State-owned Assets Supervision and Administration Commission has published in late 2018 guidelines urging large state-owned enterprises to establish comprehensive compliance programmes, and various government agencies has jointly published in late 2018 guidelines to urge enterprises involved in foreign trade and investment business to establish comprehensive compliance programmes covering issues related to trade, fair competition, anti-corruption, intellectual property, labour, etc.

Meanwhile, there are specific compliance requirements for banking financial institutions. According to the *Notice of the China Banking Regulatory Commission on Issuing the Guidelines on the Management of Country Risk by Banking Financial Institutions*, when a banking financial institution is conducting its due diligence on transaction parties, it shall strictly comply with relevant UN resolutions and remain alert on its business and transactions involving sensitive countries or regions. The compliance expectations include timely checking sanction resolutions of the UN, establishing appropriate information management systems, timely filing and updating the sanction lists and information about suspicious clients, etc. Furthermore, banks are also required to develop their “Know Your Customer” profiles for the administration of bank accounts to implement the relevant UN sanction resolutions (*Notice of the General Office of China Banking Regulatory Commission on Strengthening the Management of Bank Accounts and Effectively Implementing the Relevant Sanction Resolutions of the United Nations*).

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes. The Chinese government implements UN economic sanctions through a series of administrative notices. While the notices themselves do not provide criminal penalties for violations, specific incompliant activities nevertheless may constitute criminal violations under PRC Criminal Law. For example:

Financial transactions with sanctioned individuals/entities could be regarded as money laundering under certain circumstances. In the case of money laundering, financial institutions and other involved individuals/entities may be subject to criminal punishments under Article 191 of PRC Criminal Law, including the confiscation of illegal income and gain, fines, and imprisonment of up to 10 years.

In the case of trading of goods, importing or exporting of goods from or to sanctioned individuals/entities may be regarded as smuggling goods prohibited from import/export, which leads to severe criminal liabilities under Article 151 of PRC Criminal Law, including fines, criminal detention, imprisonment, etc.

For violations under the Anti-foreign Sanctions Law where Chinese persons fail to implement the countermeasures taken against the sanctioned persons, the violators may be held criminally liable under the Criminal Law.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

Violations initially will be investigated by the relevant regulatory authorities, such as the MFA, MOFCOM, Ministry of National Security, People's Bank of China or Customs. If the authorities find that such violations constitute criminal offences, cases are further investigated by public security organs and/or the anti-smuggling division of Customs, and prosecuted by the people's procuratorates.

4.3 Is there both corporate and personal criminal liability?

There are both corporate and personal liabilities for criminal violations. For example, if a financial institution is found guilty

of money laundering, it shall be fined, and any of the persons who are directly in charge, as well as the other persons who are directly responsible for the crime, shall be punished accordingly.

For a crime of smuggling, if the organisation/entity is punished criminally, the person in charge could be indicted and subject to imprisonment as well.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

The maximum financial penalties are dependent on the criminal activities, the gravity of the violation and the amount of illegal income. For the crimes of money laundering or of smuggling goods prohibited for import or export, the amount of financial penalty is to be decided based on the gravity of the violation and there is no maximum financial penalty specified.

4.5 Are there other potential consequences from a criminal law perspective?

Individuals/entities criminally punished could be placed on a discredited name list, which would have a wide range of consequences; for example, restrictions on excessive spending, restrictions on assuming managerial roles in an entity, stricter scrutiny in import and export, and other practical difficulties such as in obtaining financing, etc.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

Similar to criminal penalties, administrative (civil) penalties are provided in the administrative notices themselves. Specific incompetent activities can be of administrative violation under relevant laws and regulation, for example:

Financial institutions may be subject to administrative penalties if violating the Anti-Money Laundering Law. Financial institutions may be subject to fines ranging from 200,000–5 million RMB, and penalties of suspension or revocation of their business licence. Employees directly in charge may be subject to fines ranging from 10,000–500,000 RMB and be sanctioned by a disciplinary warning, be deprived of qualifications or be prohibited from engaging in relevant financial industry work.

In the case of the exporting of prohibited goods that violate relevant sanctions, an individual/company in breach of the relevant laws relating to sanctions could be subject to one or several of the following penalties: 1) revocation of a business licence; 2) confiscation of the relevant goods and illegal proceedings; 3) fines of up to 1 million RMB; and/or 4) exclusion from obtaining export licences and/or the limitation or revocation of export trading rights.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

Administrative (civil) economic sanctions violations are investigated and enforced by relevant authorities such as the General Customs of China, the People's Bank of China (the central bank), China Banking and Insurance Regulatory Commission, China Securities Regulatory Commission, the Ministry of Transport and the Ministry of Public Security, in their respective authority.

4.8 Is there both corporate and personal civil liability?

There are both corporate and personal liabilities for administrative violations. For example, in the case of money laundering, financial institutions may be subject to fines ranging from 200,000–5 million RMB and the persons in direct charge may be subject to fines ranging from 10,000–500,000 RMB, and be sanctioned by a disciplinary warning, be deprived of qualifications or be prohibited from engaging in relevant financial industry work.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

The maximum financial penalties are dependent on the activity of the violation, the gravity of the violation and the amount of the illegal income. For example, the maximum financial penalties for financial institutions in violation of anti-money laundering may be subject to fines of 5 million RMB, and their employees in charge may be subject to fines of 500,000 RMB.

4.10 Are there other potential consequences from a civil law perspective?

Individuals/entities administratively punished could be placed on a discredited name list, which would have a wide range of consequences; for example, restrictions on excess spending, restrictions on assuming managerial roles in an entity, stricter scrutiny in import and export, and other practical difficulties such as in obtaining financing, etc.

Foreign entities may also be placed onto the UEL under the UEL Provisions.

In addition, under Blocking Rules and the Anti-Foreign Sanctions Law, potential civil litigations may be brought by Chinese persons against Chinese or foreign persons who violate the law or regulations.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

Since the PRC implements UN economic sanctions through administrative notices, the administrative (civil) enforcement process differs in different laws and regulations. Taking the *People's Bank of China Administrative Penalties Procedures* as an example, an Administrative Penalties Committee is set up to conduct the major administrative (civil) enforcement. The Administrative Penalties Committee takes charge of the initiation, investigation, hearing and review of the case. Where the Committee decides to impose administrative penalties, it shall produce the "People's Bank of China Administrative Penalty Decision". The assessment of penalties depends on the gravity of the violation and the amount of the illegal income, and there is no specific guidance on penalties assessment.

The resolutions by the competent authorities are generally public on their official websites.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Persons or entities who do not accept an administrative (civil) penalty shall have the right to apply to the people's government

at the same level or to the competent department at a higher level for administrative reconsideration. In general, persons or entities may apply for administrative reconsideration within 60 days from the date when they come to know such administrative acts. The administrative organ shall examine the application to decide whether to accept the application within five days. The reconsideration decision shall be made within 60 days from the date it accepts an application.

In addition, persons/entities who does not accept an administrative penalty also have the right to directly bring an administrative lawsuit without going through the administrative reconsideration process.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal and administrative (civil) enforcements are not limited at the national level. In fact, most criminal and civil enforcement is at the local level of competent government agencies. Certain severe or high-profile cases will be escalated to provincial or even national-level government agencies.

4.14 What is the statute of limitations for economic sanctions violations?

For criminal sanctions violations, the statute of limitation is subject to a statutory maximum sentence, and ranges from five to 20 years. For administrative sanctions violations, the statute of limitations is two years from the date the illegal act is committed, while it may be extended to five years if the act causes harm to financial security. To initiate civil litigations under Blocking Rules and the Anti-Foreign Sanctions Law, the statute of limitations is three years starting from when the persons know or should have known that their rights have been infringed upon.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

All sanctions-related measures are stated above.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

As stated above, China implements the UN sanctions through a series of administrative notices. Most of notices can be found from the website of the MFA at: <https://www.fmprc.gov.cn>. The notices of the MFA are written in Chinese only and the MFA does not provide any official documents in English.

Besides, for Chinese regulations regarding economic sanctions:

- The Provisions on the Unreliable Entity List (in English): <http://english.mofcom.gov.cn/article/policyrelease/announcement/202009/20200903002580.shtml>.
- The Blocking Rules (in English): <http://english.mofcom.gov.cn/article/policyrelease/announcement/202101/20210103029708.shtml>.
- The Anti-Foreign Sanctions Law (in Chinese): <http://www.npc.gov.cn/npc/c30834/202106/d4a714d5813c4ad-2ac54a5f0f78a5270.shtml>. There is no English version.
- The sanctions of the MFA (in English): https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/.



Weiyang (David) Tang has over 20 years of experience specialised in international trade, customs, economic sanctions and export controls, and compliance-related investigations. *Chambers Global* and *Chambers Asia-Pacific* have consecutively recognised David as a leading lawyer in international trade since 2012.

David is one of the very few practitioners in China who has deep understanding and extensive experience in economic sanctions and export controls. He advises multinational clients on Chinese sanctions and export controls. In recent years he has helped many Chinese companies develop their compliance programmes for coping with U.S. sanctions and export controls, and assisted clients in assessing sanctions/export controls risks for their business involving sanctioned countries or restricted parties.

JunHe LLP
26/F HKRI Centre One HKRI Taikoo Hui
288 Shimen Road (No.1), Shanghai, 200041
China

Tel: +86 21 2208 6373
Email: tangwy@junhe.com
URL: www.junhe.com



Juanqi Jessica Cai's area of expertise is in international trade. She has over 10 years' experience in trade remedy investigations, customs investigations, export controls and international trade compliance.

Ms. Cai is versed in legislation and the policies and practices of trade remedies, including anti-dumping investigations, countervailing duty investigations and safeguard investigations in China, the United States, the European Union and other countries. She has a deep understanding of the accounting policies, ERP systems, and supply chain of companies across a wide range of industries. With an in-depth knowledge of law and accounting, Ms. Cai has had exceptional success in defending clients in their investigations.

JunHe LLP
26/F HKRI Centre One HKRI Taikoo Hui 288
Shimen Road (No.1), Shanghai, 200041
China

Tel: +86 21 2283 8253
Email: caijq@junhe.com
URL: www.junhe.com



Runyu (Roy) Liu is an associate in JunHe LLP's Shanghai Office. She specialises in trade compliance, customs and trade remedies. Roy has good knowledge of U.S. export controls regulations and sanctions regimes. She provides legal services regarding internal audits/investigations related to trade sanctions and export controls. She assists several clients in developing compliance programmes, KYC/end user due diligence and audits. Roy advises multinational clients on Chinese export controls and sanction policies.

JunHe LLP
26/F HKRI Centre One HKRI Taikoo Hui 288
Shimen Road (No.1), Shanghai, 200041
China

Tel: +86 21 2283 8247
Email: liury@junhe.com
URL: www.junhe.com



Siyu (Rain) Wang is an associate in JunHe LLP's Shanghai Office. She mainly practises in the area of U.S. sanctions and export controls. She has helped in many risk assessments for Chinese SOEs and private companies in their business involving sanctioned countries. She also helps prepared tailor-made compliance programmes for clients of different sizes and risk levels. Siyu also advises on U.S.-China trade issues, such as the 301 tariffs and Chinese retaliatory tariff measures, Chinese export controls development and countermeasures.

JunHe LLP
26/F HKRI Centre One HKRI Taikoo Hui 288
Shimen Road (No.1)
Shanghai, 200041
China

Tel: +86 21 2283 8266
Email: wangsy@junhe.com
URL: www.junhe.com

JunHe, founded in Beijing in 1989, was one of the first private partnership firms in China. Since its establishment, JunHe has grown to be one of the largest and most recognised Chinese law firms.

The firm has 10 offices around the world and a team comprising more than 680 professionals, including over 200 partners and legal counsel, as well as over 480 associates and legal translators.

JunHe is the only Chinese law firm to be admitted as a member of Lex Mundi and Multilaw, two international associations of independent law firms. JunHe and selected top law firms in major European and Asian jurisdictions are "best friends". Through these connections, we provide high quality legal services to clients doing business throughout the world.

www.junhe.com



JUNHE

君合律师事务所

France

BONIFASSI Avocats



Stéphane Bonifassi



Sinem Paksut

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

France is a member of the European Union and the United Nations. As such, France implements sanctions issued by UN resolutions and EU regulations which are binding on France.

Furthermore, France can adopt autonomous sanctions towards physical and legal persons. These measures include financial measures and the freezing of assets belonging to persons within its territory pursuant to the Monetary and Financial Code (Article L.562-2).

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The relevant government bodies that administer the sanctions regime are the French Ministry of Foreign Affairs and the French Ministry of Economy and Finance.

Other government agencies include:

- the Directorate General of Treasury: competent for financial aspects;
- the Directorate General of Customs and Excise: competent for the classification of goods;
- the Directorate General for Competitiveness, Industry and Services: competent for the classification of dual-use goods;
- the Interministerial Commission for the Study on Exportation of Armament: competent for the accreditation of war materials and similar goods; and
- the National Agency for the Security of Drugs and Health Products: competent for the accreditation for the exportation of drugs, psychotropics, micro-organisms and highly pathogenic agents.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

In accordance with the Ruling, dated 4 December 2020, the obligations of the entities subject to AML-CFT regulations are reinforced.

The said entities must detect amongst their clients those whose assets are likely to be frozen and, whenever such measures are taken by the UN Security Council, the measures must be enforced immediately and without delay, pursuant to Article L.562-3-1 of the French Monetary and Financial Code.

Additionally, under Article L.562-4-1, III of the French Monetary and Financial Code, the same entities must proceed to a reinforced internal control in order to fulfil their obligations with respect to freezing of assets.

The said entities must be particularly careful when dealing with clients whose assets are frozen. On that account, a freezing of assets in a neighbour state should be considered as a red flag.

Finally, under the new Article L.562-12 of the French Monetary and Financial Code, the cooperation and exchange between various government agencies, with respect to freezing of assets, is also reinforced.

According to the new Articles L.135 T and L.167 of the French Book of Tax procedures, the same government agencies responsible for preparing and enforcing asset freezing measures are also given direct access to certain databases of the French Tax Administration.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The EU imposes sanctions as part of its Common Foreign and Security Policy (CFSP) with unanimous consent from Member States in the Council of the EU required if proposed sanctions are to pass into EU law.

The day-to-day administration and enforcement of EU sanctions is delegated to the relevant competent authorities in each EU Member State.

The relevant competent authorities in France are the French Ministry of Foreign Affairs and the French Ministry of the Economy (for further details, see the authorities listed in question 1.2).

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes, France implements United Nations sanctions.

There are two ways for the implementation of the United Nations Security Council resolutions:

- for resolutions involving actions within the European Union's competence, a European Regulation implements the sanction on behalf of all EU States; and
- if the resolutions involve actions within the competence of a Member State, a national act must implement United Nations sanctions.

To the best of our knowledge, there are no significant ways in which France fails to implement United Nations sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

France is a member of the European Union and implements all sanctions resulting from the Union's CFSP. These sanctions take the form of a CFSP decision adopted for a limited period not longer than a year. Towards the end of the period, the EU reviews the situation.

Just like the UN resolutions, CFSP decisions can be implemented at the European level by way of a Regulation, if the decision contains actions within the competence of the European Union. If not, a national act must be enacted in France.

Most CFSP sanctions are adopted in a two-step procedure:

- Based on a proposal from the EU's High Representative, the Council of the EU adopts a decision, which, like other CFSP decisions must be unanimous (Article 31, TEU).
- The Council also adopts, by qualified majority (Article 215 TFEU), a regulation with detailed provisions for implementation, based on a joint proposal from the High Representative and the European Commission. In addition, Member States must adopt their own national rules implementing arms embargoes and visa bans, as these areas are not EU competences.

In practice, these two steps are simultaneous with the Council adopting both the CFSP decision and regulation at the same time.

The EU can also adopt measures which are not officially sanctions but play a similar role, for instance:

- Cutting off bilateral negotiations (i.e. suspension of negotiations with Russia in 2014). Bilateral talks can be cut off by an informal Council or European Council decision.
- Suspending development aids and loans (i.e. the case of Burundi in 2016). The decisions to suspend such aid are taken by the EU voting by qualified majority.
- Withdrawing trade preferences (Sri Lanka in 2017). The decision to withdraw or restore trade preferences is taken by the European Commission.

Due to France's obligations as a Member State, there are no significant ways in which it fails to implement these sanctions.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Yes, in addition to the EU's list of sanctioned individual and entities, France also maintains its own list of sanctioned individuals and entities.

The General Directorate of the Treasury maintains a consolidated list of persons (both legal and physical) who are subject to asset freezing.

The individuals and entities are added and removed by way of ministerial rulings.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

At the EU level, listed persons and entities have the possibility to challenge the Council's decision before the Court of Justice

of the European Union, pursuant to Article 275 Section 2 and Article 263 Section 4 of the Treaty on the Functioning of the European Union.

At the national level, it is possible for an individual or a legal entity to challenge its addition to a national sanctions list either by way of a judicial appeal (*recours contentieux*) or an informal administrative appeal (*recours gracieux*) before the General Directorate of Treasury.

If the informal administrative appeal is not effective, the individual or legal entity can file a suit against the ministerial ruling before the administrative tribunal of Paris.

2.6 How does the public access those lists?

The EU list of sanctioned individuals and entities is accessible via the Financial Sanctions Database of the EU, but is restricted to those who have an account: see <https://webgate.ec.europa.eu/europeaid/fsd/fsf> and <https://ecas.ec.europa.eu/cas>.

The national list of sanctioned individuals is accessible via the French Treasury's website: <https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/tout-savoir-sur-les-personnes-et-entites-sanctionnees>.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Yes, France maintains sanctions and embargoes against several countries and organisations.

A full presentation of the sanctions at EU level can be found at the EU's sanction map: <https://www.sanctionsmap.eu/#/main>.

In addition, the General Directorate of the Treasury publishes a full list of sanctions and embargoes against other countries:

- <https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques>.
- <https://gels-avoirs.dgtresor.gouv.fr/List>.

2.8 Does your jurisdiction maintain any other sanctions?

In addition to the usual sanctions and embargoes, other sanctions include national repression measures (*équipements répression interne*) as well as prohibition to enter the French territory (*interdiction de territoire*).

2.9 What is the process for lifting sanctions?

The decision to lift a sanction rests within the legal or the administrative authority which has enacted the sanction in the first place.

EU sanctions are lifted by the Council of Europe and ministerial rulings are lifted by a similar ministerial ruling.

The French National Assembly or Senate can also enact laws to lift sanctions for symbolic purposes, but such resolutions are not binding (i.e. in 2016, the French National Assembly and Senate voted the easing of sanctions against Russia).

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

France implements the European Dual Use Export Control Annex. Export licensing in France is divided between the

Ministry of Defense, which regulates munitions items, and the Ministry of Economy's Dual-Use Goods Service (SBDU).

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

As an EU Member State, France adopted the EU Blocking Regulation of 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom.

The Blocking Regulation prohibits any EU person or entity from complying with certain U.S. extraterritorial sanctions.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

The Blocking Statute prohibits compliance by EU operators with any requirement or prohibition based on the specified foreign laws.

Practically speaking, however, the Blocking Statute is not a prohibition tool. Its purpose is rather to protect EU operators, regardless of their size and field of activity by:

- nullifying the effect in the EU of any foreign court ruling based on the foreign laws; and
- allowing EU operators to recover in court damages caused by the extra-territorial application of the specified foreign laws.

If EU operators consider that non-compliance with a requirement or prohibition based on the specified foreign laws would seriously damage their interests or the interests of the Union, they can apply to the Commission for an authorisation to comply with those laws.

Such an authorisation may be granted by the Commission in specific and duly motivated circumstances, and as a derogation from the rule.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

Sanctions can be imposed both based on the nationality and the location of the transaction.

EU sanctions apply:

- within the territory of the EU, including its airspace;
- on board any aircraft or any vessel under the jurisdiction of an EU Member State;
- to any person inside or outside the territory of the EU who is a national of an EU Member State;
- to any legal person, entity or body inside or outside the territory of the EU which is incorporated or constituted under the law of an EU Member State. This also includes branches of EU companies in third countries; and
- to any legal person, entity or body in respect of any business carried out in whole or in part within the EU.

EU sanctions do not purport to have extra-territorial effect on actions outside the EU, although they do apply to EU nationals, EU companies and EU aircraft/vessels wherever located.

Autonomous French sanctions, on the other hand, are based both on the nationality and the territoriality of the parties involved.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Under Article L.562-2 of the French Monetary and Financial Code, the Minister of Economy and Finance can order the freezing of some of the funds or all funds, financial instruments and economic resources belonging to:

- individuals, legal entities or organisations which have committed, or commit, or which on account of their functions are likely to commit, a breach of UN or EU sanctions, or which facilitate or participate in such acts; and
- legal entities directly or indirectly controlled by such individuals.

A binding ministerial ruling would be issued in such case.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes. The General Directorate of the Treasury can issue two types of authorisations:

- general licence – this may be granted upon the request of the relevant financial institution or economic operator and remain effective until revoked. A general licence will grant authorisation for transactions of a specific type which would otherwise be subject to authorisation; and
- authorisations of a general nature – these are permanent authorisations which are publicised on its website under the relevant "country" section and under the applicable "national measures".

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

The ministerial ruling of 3 November 2014 on the internal control of banks makes it mandatory for banks to put in place a detection device to assure compliance with asset freezing measures.

Whenever a bank or a financial institution suspects that a particular operation is likely to contravene the asset freezing measures, by providing funds or resources to a person whose assets were frozen, it must refuse to accomplish the operation and report the matter to the General Directorate of the Treasury and the TRACFIN (the service in charge of combating illegal financial operations).

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

As mentioned in question 3.4, French banks are required to maintain a compliance programme with respect to asset freezing under the supervision of the French Prudential Control and Resolution Authority (*Autorité de Contrôle Prudentiel et de Résolution*).

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Article 459 of the French Customs Code punishes infringement of the EU Regulations as well as violations of ministerial rulings.

According to Article 459 of the Customs Code, a penalty for the violation or attempted violation of internal regulatory and legal measures, as well as regulatory measures laid down by the EU, may result in imprisonment of up to five years, confiscation of the goods and/or the means of transport used, confiscation of the goods or assets resulting directly or indirectly from the breach, and a fine equal to the minimum amount and maximum double of the amount of the violation or attempted violation.

Under Article L.574-3 of the French Monetary and Financial Code, the same penalties apply to the management and the employees of financial institutions and the institutions and persons listed in Article L.562-3 of the Monetary and Financial Code that hold or receive any funds, financial instruments or economic resources, where these circumvent their legal obligations or obstruct the implementation of relevant measures.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

Under Article 453 of the French Customs Code, the investigations are made by customs officials, other financial officers in the administration of finance having at least the grade of a controller and officials of the French judicial police.

The same Article also provides that the decision on whether to prosecute is made by the Minister of Economy and Finance. If the Minister decides to prosecute, he/she refers to the French Public Prosecutor.

4.3 Is there both corporate and personal criminal liability?

Article 459 of the French Customs Code applies to both physical and legal persons.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

Under Article 459 of the French Customs Code, physical persons convicted of a criminal sanctions violation can be punishable by a fine as a minimum equal to no less than the amount of the violation or attempted violation and, at most, double the amount of the violation or attempted violation.

In accordance with Article 131-38 of the French Criminal Code, the amount of the fine for legal entities is five times the fine specified for individuals.

4.5 Are there other potential consequences from a criminal law perspective?

Other potential consequences are confiscations (see the answer to question 4.1).

Individuals convicted of criminal sanctions violations are, furthermore, deemed unfit to being stockbrokers, and cannot be

elected as representatives or members of chambers of commerce, of commercial tribunals or tribunals competent in labour law.

Legal entities also suffer the consequences of Article 131-39 of the French Criminal Code under which courts can impose:

- the dissolution of the legal entity;
- a prohibition to exercise;
- a placement under judicial supervision;
- a permanent or temporarily closure of the legal entity;
- disqualifications from public tender;
- prohibition to make a public appeal for funds;
- confiscations; and
- the posting of a public notice of the aforementioned measures.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

No, under French law, there are no civil penalties for violating economic sanctions laws.

There are, however, administrative penalties that could be imposed by the French Prudential Control and Resolution Authority towards legal entities or natural persons.

Under Articles L.612-1 and L.561-36 of the French Monetary and Financial Code, failure of a bank or financial institution to comply with a ministerial ruling of freezing of assets can be subject to an investigation of the French Prudential Control and Resolution Authority.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

There are no government authorities responsible for investigating and enforcing civil sanctions violations.

With regards to administrative sanctions applicable to banks or financial institutions, the relevant authority is the Sanctions Commission of the French Prudential Control and Resolution Authority.

4.8 Is there both corporate and personal civil liability?

There is no civil liability with regards to violation of economic sanctions.

However, as mentioned above, under Articles L.612-1 and L.561-36 of the French Monetary and Financial Code, specific legal entities subject to anti-money laundering and counter terrorism financing regulations, such as credit institutions and financial institutions, are inspected by the French Prudential Control and Resolution Authority. For a full list of the legal persons that can be inspected, see Article L.561-2 of the French Monetary and Financial Code.

In addition, in case of violation of anti-money laundering and counter terrorism financing regulations, personal sanctions can be imposed on the directors of those legal entities.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

Under Article L.561-36-1, IV of the French Monetary and Financial Code, a legal entity can be penalised with an administrative fine that should not exceed the following two thresholds: EUR 100,000; or up to 10% of the annual turnover.

In the case of violations of anti-money laundering and counter terrorism financing regulations, directors of the legal entities can be penalised with a fine of up to EUR 5 million.

4.10 Are there other potential consequences from a civil law perspective?

Other possible sanctions include disciplinary sanctions such as the prohibition from certain operations for a limited time period, suspension of directors for a limited time period (up to 10 years), compulsory resignation of directors, partial or total withdrawal of an accreditation, or removal from the qualified persons lists.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

Considering that there is no civil penalty, there is no civil enforcement process.

As far as the abovementioned administrative sanctions are concerned, they are decided by a Sanctions Commission during a hearing, after an investigation lead by a member of the Commission.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Decisions of the French Prudential Control and Resolution Authority can be appealed before the French Administrative Supreme Court (*Conseil d'Etat*).

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal and administrative enforcements are only at the national level.

4.14 What is the statute of limitations for economic sanctions violations?

The criminal statute limitation applicable to the violation of the Customs Code is six years.

There are no legal texts with respect to the limitation period of disciplinary actions by the French Prudential Control and Resolution Authority. However, Courts highlight that the time lapse between the disciplinary failures and action should respect the fairness of the trial (see the French Administrative Supreme Court's Ruling of 7 June 2017, n°393509, *Vaillance Courtage*).

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

Currently, there are no additional economic sanctions-related measures proposed or under consideration in France.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

French sanctions laws can be found in:

- The French Monetary and Financial Code (in French): <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026&dateTexte=20170830>.
- The French Customs Code (in French): https://www.legifrance.gouv.fr/affichCode.do?jessionid==2DFCB-ECD0C1BCC7BC146E0FB3D53694D.tpdlia23v_3?idSectionTA=LEGISCTA000006122141&cidTexte=LEGITEXT000006071570&dateTexte=

Guidance can also be found on the French Treasury's website:

- The code of conduct (in French): <https://www.tresor.economie.gouv.fr/Ressources/sanctions-financieres-internationales>.
- The guidelines of the Treasury on the implementation of asset freezing measures, jointly drafted with the French Prudential Control Authority (in French): <https://www.tresor.economie.gouv.fr/Ressources/File/433077>.
- https://acpr.banque-france.fr/sites/default/files/media/2020/02/27/v2lignes_directrices_gel_des_avoirs_06_2019.pdf.

Additional guidance can be found on the EU institutions' websites:

- The European Parliament's website (in English): [http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621870/EPRS_BRI\(2018\)621870_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621870/EPRS_BRI(2018)621870_EN.pdf).
- The European Commission's website (in English): https://ec.europa.eu/fpi/what-we-do/blocking-statute_en.
- https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/blocking-statute_en.



Stéphane Bonifassi is the founder of BONIFASSI Avocats. The Paris-based firm represents victims of fraud, embezzlement, misuse of company assets, corruption and money laundering.

Stéphane Bonifassi specialises in business crime and fraud, economic sanctions, corruption, asset recovery, forfeiture and confiscation cases, as well as transnational enforcement of judgments and internal investigations.

He regularly represents individuals or companies accused of international corruption in multiple jurisdictions. He is similarly knowledgeable about the Foreign Corrupt Practices Act of the United States and similar laws of other countries.

He also frequently represents sovereign states that are victims of corruption or fraud.

He has served as president of the Criminal Law Commission of the International Association of Lawyers (UIA), as well as co-chair of the Business Crime Committee of the International Bar Association (IBA).

BONIFASSI Avocats

34 Boulevard Haussmann
75009 Paris
France

Tel: +33 1 82 28 10 80

Email: s.bonifassi@bonifassi-avocats.com

URL: www.bonifassi-avocats.com



Sinem Paksut is an Associate at Bonifassi Avocats. She specialises in white-collar and financial crime, with a focus on cross-border cases. Her practice also includes international enforcement and asset recovery.

She gained experience at several international law firms and at a French boutique firm that specialised in criminal law. In those roles, she worked on major tax fraud cases, including the first French Deferred Prosecution Agreements rendered under *Convention judiciaire d'intérêt public*. She has also gained experience in civil and commercial litigation and joined BONIFASSI Avocats in 2019.

BONIFASSI Avocats

34 Boulevard Haussmann
75009 Paris
France

Tel: +33 1 82 28 10 80

Email: s.paksut@bonifassi-avocats.com

URL: www.bonifassi-avocats.com

BONIFASSI Avocats is a French law firm specialising in international litigation, involving complex financial crimes, with a focus on fraud, economic sanctions, corruption and asset recovery.

This practice area requires proven trial experience, demonstrated investigative tactics, a sophisticated understanding of litigation tools and proceedings, and an intrinsic familiarity with mutual legal assistance issues.

While excelling in these areas, our partners and associates also bring a depth of talent, passion and international experience in:

- criminal law and procedure, in an international context;
- transnational enforcement of confiscation orders, insolvency judgments and receiverships; and
- enforcement of foreign judgments and arbitral awards.

As a small firm, we offer our clients a commitment to personal attention characterised by accessibility, responsiveness and efficiency. Yet with our

technical expertise and focus in the areas of fraud, asset recovery, corruption and white-collar crime, our experience and international reach equal that of larger law firms.

www.bonifassi-avocats.com

BONIFASSI
— A V O C A T S —

Germany

Gibson, Dunn & Crutcher LLP
EY Forensic & Integrity Services



Michael Walther
Gibson, Dunn & Crutcher LLP



Richard Roeder
Gibson, Dunn & Crutcher LLP



Meribeth Banaschik
EY Forensic & Integrity Services



Bisman Sethi
EY Forensic & Integrity Services

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Germany applies all sanctions imposed by the United Nations Security Council (“UNSC”) (“UN Sanctions”) and, as a European Union (“EU”) Member State, all sanctions are imposed by the EU (“EU Sanctions”).

Germany does not unilaterally impose sanctions. However, Germany maintains a discrete national export control regime that – in very limited circumstances – is used to impose unilateral export control measures that are sometimes referred to as “German Sanctions” externally. For details, please refer to question 2.10 below.

Germany's sanctions regime distinguishes between sanctions with a focus on a specific jurisdiction (“*Länderbezogene Embargomaßnahmen*”) and sanctions with a focus on specific individuals/entities (“*Personenbezogene Embargomaßnahmen*”). In the following, we shall refer to both as “sanctions” and use the terminology explained below.

Sanctions with a focus on a specific jurisdiction can further be divided into (full) embargoes, comprehensive sanctions and targeted sanctions. Embargoes, as the term is used herein thereafter, prohibit all trade with or for the benefit of the sanctioned party. Comprehensive sanctions prohibit most forms of trade with or for the benefit of the sanctioned party. Targeted sanctions prohibit only specific forms of trade with or for the benefit of the sanctioned party.

Embargoes and comprehensive sanctions are regularly implemented in the form of economic sanctions. Targeted sanctions may also be implemented in the form of economic sanctions but more often than not, are implemented in the form of financial sanctions.

Economic sanctions, broadly comparable to U.S. sectoral sanctions, are designed to restrict trade, usually within a particular economic sector, industry or market – e.g., the oil and gas sector or the defence industry (“**Economic Sanctions**”).

Financial Sanctions, broadly comparable to U.S. Specially Designated Nationals (“SDN”) listings, are restrictive measures taken against specific individuals or entities that may originate from a sanctioned country or may have committed a condemned activity (“**Financial Sanctions**”).

These natural persons and organisations are identified and listed by the EU in the EU Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions (“**EU Consolidated List**”) (see question 2.4 below for details), resulting in targeted restrictions. With the application of EU Financial Sanctions, all funds and economic resources belonging to, owned by, held by or controlled by natural or legal persons,

entities and bodies listed are frozen. Moreover, no funds or economic resources can be made available, directly or indirectly, to or for the benefit of the listed parties. Finally, the knowing and intentional participation in activities intended to circumvent the EU Sanctions is also prohibited.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The government agencies that administer or enforce EU Sanctions and the German export control regime in Germany are:

- (i) the German Federal Bank (“*Deutsche Bundesbank*”), the competent authority for administering Financial Sanctions;
- (ii) the Federal Office for Economic Affairs and Export Controls (“*Bundesamt für Wirtschaft und Ausfuhrkontrolle*” (“**BAFA**”)), the competent authority for administering Economic Sanctions and the export control regime;
- (iii) the Public Prosecutor's Office (“*Staatsanwaltschaft*”), the competent authority to enforce breaches of sanctions amounting to a crime; and
- (iv) the German Customs Administration (“*Zoll*”), the competent authority to, *inter alia*, enforce breaches of sanctions that constitute an administrative offence.

Furthermore, the Federal Office for the Protection of the Constitution (“*Bundesamt für Verfassungsschutz*”) (“**BfV**”), in close cooperation with the domestic intelligence services of the German federal states and with other agencies, including BAFA, is responsible for uncovering any activities of proliferation concern in order to prevent any illegal procurement efforts of foreign countries. Also, the Financial Intelligence Unit (“**FIU**”), the central office for financial transaction investigations, organised as part of the German Customs Administration system, analyses suspicious activity reports under the Money Laundering Act, that include the overlapping topic of terrorist financing.

Finally, the EU Commission is the competent authority for certain sanctions-related authorisation requests.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

Yes.

The EU has introduced further EU Sanctions, both Economic Sanctions and Financial Sanctions, against those deemed to be responsible for, *inter alia*, the crackdown by Belarusian security forces on protesters, democratic opposition and journalists.

Further, on December 7, 2020, the EU established the EU's first global and comprehensive human rights sanctions regime (“**EU Human Rights Sanctions**”).

The EU Human Rights Sanctions allow the EU to target individuals and entities responsible for, involved in or associated with serious human rights violations and abuses, and provides for the possibility to impose travel bans, asset freeze measures and the prohibition of making funds or economic resources available to those designated.

One noteworthy case law, the German Federal Court of Justice (“*Bundesgerichtshof*”) (“*BGH*”) decided on August 31, 2020, that the procurement of materials for a foreign intelligence service, while circumventing EU Sanctions, fulfils the elements of a crime under section 18 para. 7 No. 1 of the Foreign Trade and Payments Act (“*Außenwirtschaftsgesetz*”) (“*AWG*”). Espionage or affiliation with an intelligence service is not necessary to act “*for the intelligence service of a foreign power*”.

In the case, a man sold machine tools to Russian companies for around EUR 8 million in seven cases between 2016 and 2018. The man’s actual contractual partner – a member of a Russian intelligence service – subsequently supplied the machines to a Russian state-owned arms company for military use. The arms company operates in the field of carrier technology and develops cruise missiles. The machine tools are considered dual-use technology, and the sale and export of such items to Russia has been prohibited since 2014 under the EU Russia Sanctions, specifically Regulation (EU) 883/2014 as amended.

The BGH decided that it is sufficient if the delivery of the machines is a result of the perpetrator’s involvement in the procurement structure of foreign intelligence services. An organisational integration of the perpetrator into the foreign intelligence service is not required to justify the higher penalty of section 18 para. 7 No. 1 AWG (imprisonment of not less than one year) compared to the regular sentencing range of section 18 para. 1 AWG (imprisonment from three months up to five years) imposed for embargo violations under the AWG.

Regarding the discussion around the extraterritorial U.S. sanctions against the Nord Stream II project and the European and specifically the German reaction to it, a recent agreement between the U.S. and Germany eased respective tensions.

At the same time, the broader discussion on defending the EU’s and Germany’s sovereignty, specifically on foreign policy and trade-related issues remains prevalent, as a recent respective study of the European Parliament shows. Specifically, on January 19, 2021, the EU Commission published a Communication to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions titled “*The European economic and financial system: fostering openness, strength and resilience*” as a “*key instrument*” playing a “*critical role in upholding the EU’s values and in projecting its influence internationally*”.

Following-up on the above, the EU Commission now announced that “*it would consider amending the Blocking Statute (Regulation 2271/96), to further deter and counteract the unlawful extra-territorial application of sanctions to EU operators by countries outside the EU.*” In such announcement, the EU Commission included what it could envisage, stating, *inter alia*: “*(...) the proposed regulation could envisage the award of financial or other types of support to EU operators willing to engage in trade that is prohibited by such extra-territorial sanctions of third countries but not prohibited by Union law(...).*”

2 Legal Basis / Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Germany does not unilaterally impose sanctions, but applies all UN and EU Sanctions, see question 1.1 above.

The legal authority for EU Sanctions is article 29 of the Treaty on the EU (“**TEU**”) (in the case of arms embargoes) and article 215 of the TEU (in the case of Economic and Financial Sanctions).

In the case of arms embargoes, the Council of the EU (the “**Council**”), the institution representing the governments of the EU Member States, adopts a respective decision as part of its Common Foreign and Security Policy (“**CFSP**”). This decision is binding on EU Member States, which, in turn, implement the decision on an EU Member State level. In Germany, the legal authority for such implementation and enforcement is the Foreign Trade and Payments Act (“**AWG**”), flanked by the administrative authority, the Foreign Trade and Payments Regulation (“**AWV**”).

In the case of EU Economic Sanctions and EU Financial Sanctions, the Council again adopts a respective decision as part of its CFSP and, additionally, an EU Sanctions regulation which is directly applicable in all EU Member States. While the EU Member States thus do not need to implement such EU Sanctions regulations in national EU Member State law, the EU Sanctions regulations require the EU Member States to create authorities to assure enforcement of the EU regulation on an EU Member State level.

Regarding the legal authorities or administrative authorities for implementing UN sanctions, please see question 2.2 below.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes.

United Nations (“**UN**”) Sanctions are regularly implemented via EU Sanctions that in turn apply in Germany, see question 2.1 above.

As the process of the implementation of UN Sanctions via EU Sanctions may cause a delay between listing by the UN and applicability in Germany, Germany additionally directly implements UN Sanctions based on section 6 para. 1 AWG in connection with section 4 para. 1 No. 2 and 3 AWG in connection with section 4 para. 2 No. 3 AWG and section 13 para. 6 AWG.

There are no significant ways in which the EU and/or Germany have failed to implement UN Sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

Yes.

Germany is a Member State of the EU and implements EU sanctions, see question 2.1 above. Regarding the process of implementation in the case of arms embargoes, EU Economic Sanctions and EU Financial Sanctions, the Council adopts a respective decision as part of CFSP. In Germany, the legal basis for implementation into German law and respective enforcement of such decision is the AWG, flanked by the administrative authority AWV.

In the case of EU Economic Sanctions and EU Financial Sanctions, the respective additional EU Sanctions regulation is directly applicable in all EU Member States. Therefore, while the EU Member States do not need to implement such EU Sanctions regulations in national EU Member State law, the EU Sanctions regulations require EU Member States to implement authorities to assure enforcement of the EU regulation on an EU Member State level, in Germany via the AWG, flanked by the administrative authority AWV.

There are no significant ways in which Germany has failed to implement EU Sanctions.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Germany does not maintain a list of sanctioned individuals and entities, but applies the EU Consolidated List. For the process of the implementation of such EU Financial Sanctions, see questions 2.1 and 2.3 above; for further details on (de-)listing, see <https://www.consilium.europa.eu/en/policies/sanctions/adopti-on-review-procedure/>.

Individuals and entities are added to or removed from the EU Consolidated List upon a proposal of the High Representative of the EU for Foreign Affairs or an EU Member State. Various bodies and committees of the Council discuss the respective proposal before the Council decides on the addition/removal by unanimous vote.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Sanctioned persons may submit a request to the Council, asking for the reassessment of the listing decision (see here for details: <https://www.consilium.europa.eu/en/policies/sanctions/adopti-on-review-procedure/>).

According to articles 275 and 263 of the Treaty of the Functioning of the EU, sanctioned persons may also challenge the Council's listing decision before the EU General Court of the European Union.

The European Court of Justice (“ECJ”) may also review whether UNSC Sanctions, specifically those related to listings, are in accordance with EU primary law. For illustration purposes, a respective judgment can be found at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CEL:EX:62005CJ0402&from=DE>.

2.6 How does the public access those lists?

The sanctions search tool maintained by the EU, the so-called “EU Sanctions Map” (available at <https://www.sanctionsmap.eu>), serves as a good starting point for an initial assessment on whether Germany maintains sanctions against a particular jurisdiction, individual or entity.

An overview of sanctions with a focus on specific jurisdictions can be found at https://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_embargo_uebersicht_laenderbezogene_embargos.pdf?__blob=publicationFile&v=6.

An overview of sanctions with a focus on specific individuals/entities, the so-called EU Consolidated List of persons, groups and entities subject to EU Financial Sanctions, can be found at <https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions>. Accessing search links however, from a Business As Usual (“BAU”) standpoint can be a cumbersome task, especially as sanctions screening should be performed at both the onboarding phase of a transaction or relationship, and should also continue to be monitored throughout the relationship cycle. Therefore, most companies often rely on external vendors and third parties with compliance expertise, to provide leading technology led screening solutions. The integration of sanctions screening solutions that combine technology and advanced analytics can facilitate faster screening and monitoring for review and reporting requirements.

How can companies manage those lists?

Companies often must rely on external vendors and third parties with compliance expertise to provide leading technology and screening solutions. Sanctions screening should be performed at the onboarding phase of a transaction or relationship, and ongoing monitoring should continue throughout the relationship cycle. While screening at the onboarding stage appears straightforward, one of the key challenges can be adopting an automated screening system integrated with the organisation's onboarding systems including, *inter alia*, Enterprise Resource Planning (“ERP”), Customer Relationship Management (“CRM”) and Human Resources (“HR”) systems. The integration of screening solutions that combine technology and advanced analytics can facilitate faster screening and monitoring for review and reporting requirements.

What does ongoing monitoring involve and what is its relevance to businesses?

Ongoing monitoring includes a review of an organisation's relevant key data sets against any new updates to the sanctions watch lists. Ongoing monitoring ensures that business activities are up to date and in line with the risk assessment conducted at the time of onboarding. Many companies automate this procedure, to check for changes in politically exposed person (“PEP”) status, penalties, and negative publicity on a regular basis. They monitor any changes in customer risk and exposure by screening against dynamic, up-to-date global databases. This process also takes into consideration records where key know-your-customer (“KYC”) attributes such as address, nationality and other personal identification indicators may have been updated as a part of the organisation's anti-money laundering (“AML”) KYC refresh regime.

The global economic and financial landscape has shifted dramatically as a result of the COVID-19 pandemic. On one hand, increased unemployment has prompted unscrupulous actors to commit financial crime through charity organisations, digital e-wallet platforms and cryptocurrency exchanges, exposing businesses to a higher risk of money laundering and terrorist financing creating the need for a more robust ongoing monitoring framework. While most screening systems and solutions today support automated ongoing review requirements, there is significant operational optimisation that can be achieved through effective technology system configurations. This includes review and mapping of the organisation's data with the corresponding data available in the watch lists. A well-tuned technology solution will assist the organisation in reviewing potential matches through a framework that can support internal system integrations and real-time triggers based on automated watch lists updates.

Automated ongoing monitoring can assist businesses with monitoring the risk profiles of their customers and third parties, while not changing in a way that exposes the firm to non-compliance and reputation damage. Organisations greatly benefit from conducting ongoing risk assessment of their business relationships, which include the primary engaging entity (“customer” and or “third party”), its ultimate beneficiary ownership (“UBO”) and senior management (“SM”) officials. The primary customer along with the key associations (UBOs and SMs) are then reviewed on a watch list, belonging to a sanctioned country or a high-risk industry.

What causes higher false positives and how can organisations manage false positives better?

One of the top reasons of higher false positives is continued reliance on rule-based screening engines. While technology for name screening evolves rapidly, the issue of false positives is still

seen as one of the top challenges organisations face to accurately detect true screening matches. It is observed in most legacy systems that screening rules are built to scan customer data fields, not available on the watch list dataset. This would include running screening rules in combination with data such as date of birth, address, and passport information. This, however, can benefit only to the extent that this information is available on the watch list dataset, which unfortunately is not the case for a large percentage of records in the watch list data, resulting in higher false positives, due to the missing variable elements.

Another leading reason for increased false positives is the quality of data used for the screening. It is observed that the gaps in the data capture design requirements, which increases the chances of errors in the data capture process, and can therefore increase the risk of false positives and false negatives occurring.

Many advanced screening solutions offer capabilities based on natural language processing (“NLP”) technologies in machine learning to optimise false positives. The NLP technology assists organisations to read unstructured data and determine its meaning in the screening process. Organisations are now looking at a hybrid approach to achieve enhanced false positive optimisation. The hybrid approach includes technology functions that optimise the potential matches based on variations in word boundaries, native character variations (such as “ö” to “oe”), extra words or spelling errors in commonly found names, which are often caused by unintentional error(s) or introduced intentionally to evade detection. Advanced screening tools also use a combination of match screening algorithms that are tuned using the organisations historical, manually conducted false positive screening reviews. Another functionality that can assist organisations to optimise false positives is effective “whitelisting”. This feature can allow organisations to list entities that could be exempted from the screening process.

False positive optimisation is increasingly important as it can help manage customer onboarding and transaction experience, without compromising on the effectiveness of the AML compliance requirements. Effective management of false positive matches may also reduce the likelihood of breaching other areas of law such as the principle of data minimisation or data accuracy in article 5 of the EU General Data Protection Regulation (“GDPR”).

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

For an explanation of the different types of sanctions, please see question 1.1.

The UN, the EU and, correspondingly, Germany currently do not apply embargoes against any country or region.

However, North Korea is currently subject to comprehensive sanctions and the Crimea Region is currently subject to a broad set of targeted sanctions.

2.8 Does your jurisdiction maintain any other sanctions?

Germany, as of August 11, 2021, applies sanctions targeting CFSP concerns specifically related to 33 non-EU countries: Afghanistan; Belarus; Bosnia and Herzegovina; Burundi; Central African Republic; China; Democratic Republic of the Congo; Guinea; Guinea-Bissau; Haiti; Iran; Iraq; Lebanon; Libya; Mali; Moldova; Montenegro; Myanmar (Burma); Nicaragua; North Korea; Russia; Serbia; Somalia; South Sudan; Sudan; Syria; Tunisia; Turkey; Ukraine; United States; Venezuela; Yemen; and Zimbabwe.

2.9 What is the process for lifting sanctions?

The same procedure for the imposition of sanctions applies to the revocation of sanctions; please refer to question 2.1 above.

Accordingly, the decision by the Council must also be unanimous. This requirement has led to the fact that EU Sanctions regulations often contain an end date, so that instead of a uniform decision to lift them, a uniform decision to maintain the sanctions will usually be required every six months.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes.

Germany maintains a discrete and complex national export control regime. The German export control regime is regulated by the AWG. The AWG governs both the transfer to EU Member States and the export to non-EU Member States of certain goods.

The German export control regime implements requirements from the relevant international agreements, such as the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australian Group and the Missile Technology Control Regime. It is a discrete national regime, yet Germany regularly aligns with the CFSP, specifically via the EU Dual Use Regulation and the EU Common Military List.

On the EU Dual Use Regulation, in order to keep up with the latest technological developments and to mitigate national security concerns, on May 10, 2021, the Council of the EU adopted a regulation that, by recasting Council Regulation (EC) No. 428/2009 (the “*EU Dual-Use Regulation*”), not only modernises, but also substantially expands the scope and breadth of the EU system for the control of exports, brokering, technical assistance, transit and transfer of dual-use products and technologies (the “*New EU Dual-Use Regulation*”).

The New EU Dual-Use Regulation will: (i) strengthen controls on a wider range of emerging dual-use technologies, including cyber-surveillance tools, that can be used for both civilian and military applications; (ii) introduce due diligence obligations and compliance requirements for exporters, recognising the role of the private sector in addressing the risks posed by trade in dual-use items to international security; and (iii) increase the coordination between Member States and the EU Commission in support of the effective enforcement of controls throughout the EU.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions’ sanctions or embargoes?

Yes.

Germany enforces the EU Blocking Statute (as amended, the “*EU Blocking Statute*”), and the AWV also includes the prohibition against declaring adherence to a foreign boycott. Further, the GDPR, while having the primary function of protecting the personal data and privacy rights of EU data subjects in practice, can sometimes act as a “Blocking Statute” prohibiting transfers to non-EEA countries or the processing of personal data pursuant to obligations that arise outside of EU or EU Member State law.

EU Blocking Statute

On August 6, 2018, the EU enacted Commission Delegated Regulation (EU) 2018/1100, which amended Council Regulation

(EC) No. 2271/96. The effect of the EU Blocking Statute is to prohibit compliance by EU entities with, *inter alia*, the re-imposed U.S. sanctions on Iran as well as certain U.S. sanctions on Cuba, most relevant are those deriving from the application of certain parts of the U.S. Cuban Liberty and Democratic Solidarity Act of 1996, the so-called “Helms-Burton Act”.

The EU Blocking Statute was originally enacted in 1996 as a countermeasure to certain U.S. extraterritorial sanctions against Cuba, Iran and Libya. The EU viewed these sanctions as a violation of international law, a threat to international trade, and an impairment of the interests of “EU Operators”. Consequently, pursuant to its preamble, the regulation sought to protect against the “effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom”. To achieve that goal, the statute, *inter alia*, prohibits compliance with any legal acts listed in the regulation which “purport to regulate activities of natural or legal persons under the jurisdiction of a Member State”. The Member States of the EU are responsible for implementing sanctions to be imposed in the event of a breach. Germany does so by penalising a breach of the EU Blocking Statute as an administrative offence with a maximum fine of EUR 500,000 with the potential of additional forfeiture of gains.

In addition, the EU Blocking Statute nullifies the effect of foreign court judgments based on these legal acts in the EU, hinders service and discovery requests, such as those deriving from Helms-Burton Act claims and establishes a reporting obligation as well as a right to recover damages. These effects and obligations have been discussed in depth at <https://www.gibsondunn.com/new-iran-e-o-and-new-eu-blocking-statute-navigating-the-divide-for-international-business/>.

Boycott Declaration Prohibition

Section 7 of the AWV states: “*The issuing of a declaration in foreign trade and payments transactions whereby a resident participates in a boycott against another country (boycott declaration) shall be prohibited (...)*”

There is no precedent clarifying the exact scope, but it is a common understanding among sanctions practitioners in Germany that, unlike the EU Blocking Statute, section 7 of the AWV does not prohibit mere compliance with foreign sanctions; rather, it specifically prohibits the *issuing of a declaration* to do so.

On December 19, 2018, section 7 of the AWV was amended, clarifying that “[*The boycott declaration prohibition*] shall not apply to a declaration that is made in order to fulfil the requirements of an economic sanction by one state against another state against which the Security Council of the United Nations in accordance with Chapter VII of the United Nations Charter, the Council of the European Union in the context of Chapter 2 of the Treaty on European Union or the Federal Republic of Germany has also imposed economic sanctions”.

This revision only leaves a narrow window of application of section 7 of the AWV. As an example, due to no UN, EU and, accordingly, German Sanctions implemented or applied against Cuba, the issuing of a boycott declaration relating to Cuba in the context with a German nexus should be approached carefully.

General Data Protection Regulation

Sanctions screening involves screening customer data against designated sanction lists. The very act of inputting a name (or, indeed, other details such as address, nationality, passport, tax ID, place of birth, date of birth, former names and aliases) into a sanctions screening tool or the filing of a Suspicious Activity Report (“SAR”) could qualify as an act of personal data processing under the GDPR.

The processing of personal data is lawful under the GDPR when conducted in line with one of the legal bases provided in the regulation, such as when it is “(...) necessary for compliance with a

legal obligation to which the controller is subject (...)” as per article 6(1) (c) of the GDPR. While a German company may be able to rely on EU sanctions law as a “legal obligation” justifying the screening of personal data under some circumstances, this may not necessarily be the case for sanctions screening due to U.S. and other third-country sanctions, export control laws and regulations – which stems from a “legal obligation” arising outside of EU or EU Member State law.

Further, the “*Schrems II*” judgment (CJEU Case C-311/18) on July 16, 2020 invalidated the EU-US Privacy Shield and consequently put into doubt the legality of personal data transfers to the United States without additional safeguards. However, for now, personal data that is transferred to courts, tribunals, and administrative authorities outside the EEA (pursuant to a mutual legal assistance treaty or equivalent) or under an article 49 GDPR derogation do not seem to be affected by the judgment. In practice what this means is that German companies should continue to monitor this area of the law for potential developments.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as “Secondary Sanctions”)?

No, however, please note that EU Sanctions regularly apply to businesses carried out in whole or in part in the EU.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction’s sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

Broadly speaking, any parties and transactions with a nexus to Germany and/or the EU may be subject to sanctions as well as export control laws and regulations applicable in Germany.

In Germany specifically, any trade in goods, services, capital, payments and other types of trade with foreign (*i.e.*, non-German) territories, as well as the trade in foreign valuables and gold between residents of Germany (“*Außenwirtschaftsverkehr*”), while not restricted *per se*, is subject to Germany’s sanctions and export control laws and regulations, specifically to the restrictions of the AWG and AWV.

This also includes restrictions of international agreements, which the German legislative bodies have approved in the form of federal acts, such as the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australian Group and Missile Technology Control Regime, and legal provisions of the bodies of international organisations to which the Federal Republic of Germany has transferred sovereign rights (*i.e.*, the EU).

EU Sanctions, in turn, generally apply: (i) within the territory of the EU; (ii) on board any aircraft or vessel under the jurisdiction of an EU Member State; (iii) to any person inside or outside the territory of the EU who is a national of an EU Member State; (iv) to any legal person, entity or body, inside or outside the territory of the EU, which is incorporated or constituted under the law of an EU Member State; and (v) to any legal person, entity or body in respect of any business done in whole or in part within the Union (for more information, please refer to the factsheet for EU restrictive measures, available at https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/135804.pdf).

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Yes.

Any individual or entity obliged to comply with EU Financial Sanctions, regularly EU banks and financial institutions, that know or have reasonable cause to suspect that they are in control or in possession of, or are otherwise dealing with, the funds or economic resources of a person subject to EU Financial Sanctions, must (i) freeze the funds and specifically not deal with them or make them available to, or for the benefit of, the designated person, and (ii) report the funds or economic resources to the competent authority of the EU Member State (in Germany, the Federal Bank). See question 3.4 for further details on reporting.

Making payments to a bank account of a sanctioned person is prohibited, unless specifically authorised by competent authority or unless it is reasonably determined that the funds will not be made available to the sanction person. EU banks may credit frozen accounts insofar it can be ascertained that the incoming funds are frozen upon being credited to the account.

For specific questions on freezing of funds and/or making available economic resources, please see the respective Commission opinion of June 19, 2020, available at https://ec.europa.eu/info/sites/info/files/200619-opinion-financial-sanctions_en.pdf.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes.

For EU Financial Sanctions, e.g., based on *Council Regulation (EU) 269/2014 of March 17, 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine* as amended, the competent authorities of the EU Member State to enforce such EU Financial Sanctions (in Germany, the Federal Bank) may authorise the release of certain frozen funds or economic resources, or the making available of certain funds or economic resources, after having determined that the funds or economic resources concerned are necessary to satisfy the basic needs of the sanctioned person or if the funds or economic resources concerned are intended exclusively for payment of reasonable professional fees or reimbursement of incurred expenses associated with the provision of legal services.

For EU Economic Sanctions, e.g., based on *Council Regulation (EU) 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine* as amended, the competent authorities of the EU Member State to enforce such EU Economic Sanctions (in Germany, BAFA) may authorise certain transactions, e.g., the sale of certain items for use in Russia used for oil exploration and production in waters deeper than 150 metres.

For specific licences related to the EU Blocking Statute, the respective request should be sent to the EU Commission's dedicated EU Blocking Statute team at: EC-AUTHORISATIONS-BLOCKING-REG@ec.europa.eu.

The German export control regime also includes exceptions and authorisation requirements. A more detailed description on the respective process can be found at https://www.bafa.de/EN/Foreign_Trade/Export_Control/export_control_node.html.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Yes.

According to the respective provisions of EU Financial Sanctions, e.g., *Council Regulation (EU) 269/2014 of March 17, 2014*, those who are subject to EU Financial Sanctions must: supply immediately any information which would facilitate compliance with the Regulation to the competent authority of the EU Member State authority, in Germany accordingly, to the Federal Bank; must transmit such information to the EU Commission; and must cooperate with the competent authority.

Further, there are additional reporting obligations in place, e.g., financial institutions, traders of goods, notaries, lawyers, auditors, tax consultants and real estate professionals are all required to report suspicious activities and transactions. Such organisations are expected to report information about sanctioned individuals through reporting of SARs, or Suspicious Activity Reports. These must be reported to the Deutsche Bundesbank, which is responsible for the implementation of EU Regulations on Financial Sanctions in Germany, and/or the FIU. Specifically, in case of asset freezes due to EU Financial Sanctions, banks and financial institutions must provide information about any funds, accounts, assets, BIC codes, reference numbers, amounts and dates connected with the sanctioned individuals and entities.

How can technology support regulatory reporting?

Advanced screening tools can facilitate automated regulatory reporting. The identified suspicious sanctions activity is reviewed through a case management workflow. Once the required information is consolidated and review remarks are updated, the system enables consolidation of information in the requisite regulatory reporting format. The goal is to reduce errors that may arise on account of multiple manual entries. This use of technology also has the added benefit that it can enable an audit trail for the reported information, which is particularly useful if a sanctions lookback needs to be conducted.

In addition to the above, many organisations apply “Robotics Automation” for the elimination of the excessive manual touchpoints in the sanctions review processes and information consolidation requirements. This can assist organisations in increasing operational efficiencies, reduce sanctions review timelines and applicable costs.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

Both the EU, via EU Commission guidance (see <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&from=EN> and <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2018.277.01.0004.01.ENG&toc=OJ:C:2018:277I:TOC>), and the German government, via BAFA (see http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3), have recently become more vocal on how they expect individuals and companies under their jurisdiction to implement sanctions and export control laws and regulations.

In principle, while there is no obligation to maintain a compliance programme, the responsible persons must prove “the due care of a prudent manager faithfully complying with his

duties”, see http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3 (referring to section 93 of the German Stock Corporation Act), which will be – to say the least – facilitated by maintaining a risk-based compliance programme.

The guidance provided by the EU Commission and BAFA is similar and suggests that management, in the area of sanctions and export control, set up an internal export control programme, which should include the following components: a regularly repeated risk assessment; management commitment to the objectives of sanctions and export control compliance; an organisational structure and distribution of responsibilities reflecting the results of the risk assessment; sufficient human and technical resources and other (IT) work equipment to address the identified risks; appropriate process organisation; record-keeping and storage of documents; diligent staff selection, training and awareness raising, as well as regular reviews of process and system controls (ICP audits), taking appropriate corrective actions if the need may be; the establishment of a whistle-blower system; and assuring physical and technical security.

It is observed that leading organisations focus on specific risk factors such as geographic locations of business operations, risks posed by third parties, suppliers, and their intermediaries, along with the specific risks posed by product and services. Organisations are keen to put in place a comprehensive root cause analysis (“RCSA”) framework, for the deficiencies identified in the control testing process.

Continuous review mechanisms around the recent global sanctions enforcement actions are also key to account for any policy related updates required. This may also assist how businesses prioritise their risk assessment programmes. One such business area, for instance, could include mergers and acquisitions, where businesses need to carry out more detailed due diligence exercises regards sanctions risk assessments of the primary and associated entities of the new business relationship.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes.

Violations of EU Sanctions and German foreign trade law, including Germany’s export control regime, may be punished as criminal offences or as administrative offences.

Intentional violations constitute criminal offences. According to section 17 para. 1 AWG, for example, a violation of an arms embargo constitutes a criminal offence and is punishable by imprisonment of up to 10 years. Furthermore, a fine may be imposed and determined according to the offender’s individual financial situation/income and the offence.

Negligent violations of EU Sanctions and German foreign trade law, including Germany’s export control regime, are generally considered administrative offences. “Negligence” is defined as not exercising the necessary standard of care (“*Fahrlässigkeit*”). As per section 19 para. 6 AWG, such administrative offence may result in a fine of up to EUR 500,000 per offence and forfeit of gains resulting from the administrative offence committed.

Further details can be found at http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The authority responsible for investigating and prosecuting criminal Economic Sanctions is the public prosecutor’s office at the court which exercises local jurisdiction over the breach of sanctions (section 143 para. 1 of the Courts Constitution Act (“*GVG*”)).

The competent public prosecutor’s office will be assisted by the competent authority administering the sanctions (in case of Financial Sanctions, the Bundesbank, and in case of Economic Sanctions, the BAFA); see question 1.2 above.

Only in rare and extremely exceptional cases may the Federal Prosecutor General take over the investigation (section 142a *GVG*); e.g., if the sanctions violation investigated has the potential to disrupt or endanger national security or external security of the foreign relations of the Federal Republic of Germany.

4.3 Is there both corporate and personal criminal liability?

Yes.

While the concept of corporate criminal liability does not exist under German law, corporations still may face administrative penalties based on the Act on Regulatory Offences (“*OWiG*”).

Specifically, under section 30 *OWiG*, the corporation may be fined if certain executive employees, specifically executive employees with the power to represent the corporation, have committed a criminal offence or a regulatory offence, e.g., a breach of applicable sanctions laws and regulations, as a result of which duties incumbent on the corporation have been violated, or where the corporation has been enriched or was intended to be enriched.

Furthermore, under section 130 *OWiG*, if the owner or certain executive employees, specifically executive employees with the power to represent the corporation, intentionally or negligently omit to take the supervisory measures required to prevent contraventions, e.g., breaches of applicable sanctions laws or regulations, such owner or executive employee may be held liable. An example of this would be the failure to implement an effective internal compliance programme resulting in a breach of sanctions laws or regulations by an employee whom the owner or the executive employee was supposed to supervise.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

In general, and if a maximum fine is not specified in the particular law, the maximum fine for individuals should not exceed EUR 1,000, section 17 para. 1 *OWiG*. However, section 19 para. 4 AWG punishes administrative offences of individuals in the context of sections 19 para. 1, para. 3 No. 1 lit. a, para. 4 sentence 1 No. 1 with a maximum fine of up to EUR 500,000. Other administrative offences regarding the AWG are to be punished with a maximum fine of up to EUR 30,000. The exact amount depends on the economic circumstances of the offender.

According to section 30 para. 1 *OWiG*, if the institution or a member of the institution authorised to represent a legal entity, the executive or a member of the board of directors of an association, a shareholder authorised to represent a legal entity or any other executive commits a criminal or administrative offence which violates the responsibilities of or enriches or was supposed

to enrich the legal entity, it – this means the legal entity itself – can be punished with an administrative penalty. In the case of an intentional criminal offence, a fine of up to EUR 10 million can be imposed; in the case of a negligent criminal offence, a fine of up to EUR 5 million can be imposed (section 30 para. 2 sentence 1 OWiG). If the violation in the context of section 30 para. 2 OWiG is an administrative offence, the maximum fine is governed by the particular violated law, section 30 para. 2 sentence 2 OWiG. If the particular law governing the administrative offence refers to section 30 para. 2 sentence 3 OWiG, the maximum fine multiplies by 10.

In any case, the maximum fine can be significantly higher if section 17 para. 4 sentence 1 OWiG is applicable. Section 17 para. 4 sentence 1 OWiG states that the fine is supposed to be higher than the economic advantage for the offender. According to section 17 para. 4 sentence 2 OWiG, every particular maximum fine can therefore be exceeded significantly if the economic advantage for the offender is higher than the maximum fine. Section 17 para. 4 sentence 1 OWiG is also applicable regarding fines according to section 30 para. 1 OWiG, section 30 para. 3 OWiG.

4.5 Are there other potential consequences from a criminal law perspective?

Yes.

As further consequences of a violation of sections 17, 18, 19 AWG, objects to which the offence or administrative offence relates, and objects that were used or intended for their commission or preparation, may be confiscated pursuant to section 20 AWG.

In practice, a breach has practical consequences with regard to the customs authority. In response to a breach, the customs authority may suspend or revoke authorisations or customs simplifications that have been granted. The consequences particularly affect export-oriented companies. Finally, the audits carried out by a customs authority depend on the risk profile of the company. Thus, if the customs authority has noticed an increase in the number of infringements committed by the company in foreign trade and has already imposed fines, the frequency of the company's audit automatically increases.

As a further potential consequence, according to section 124 I No. 3 GWB, contractual authorities may exclude a company from participating in any award procedure if the company has committed serious misconduct while doing business questioning its integrity. As the awarding authority has scope for assessment when determining if a company has committed serious misconduct questioning its integrity, possibly a violation of sections 17, 18, or 19 AWG, this could lead to an exclusion according to section 124 para. 1 No. 3 GWB.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

Yes.

The AWG also provides for civil law consequences of a negligent violation against economically imposed sanctions. The requirements for a fine are found in section 19 para. 1 AWG in connection with 18 para. 1 AWG. Furthermore, as an example, the courts might find a termination void and, therefore, unenforceable in case such termination was itself a breach of the EU Blocking Statute. See question 2.11 above.

4.7 Which government authorities are responsible for investigating and enforcing civil Economic Sanctions violations?

The local public prosecutor's office and customs, with assistance of the Bundesbank and BAFA, are responsible. See question 1.2 above.

4.8 Is there both corporate and personal civil liability?

Yes, see question 4.3 above.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

According to section 19 para. 6 AWG and section 30 para. 2 OWiG, a fine may be imposed up to a maximum of EUR 500,000. It should be noted that section 17 para. 4 OWiG provides the possibility to impose fines higher than the maximum fines regulated by law in cases where the economic benefit which the offender received is greater than the maximum fine regulated by law ("*disgorgement*").

However, the maximum fine can be significantly higher if section 17 para. 4 No. 1 OWiG is applicable. Section 17 para. 4 No. 1 OWiG states that the fine is supposed to be higher than the economic advantage for the offender. According to section 17 para. 4 No. 2 OWiG, every particular maximum fine can therefore be exceeded significantly if the economic advantage for the offender is higher than the maximum fine. Section 17 para. 4 No. 1 OWiG is also applicable regarding fines according to section 30 para. 1 OWiG and section 30 para. 3 OWiG.

4.10 Are there other potential consequences from a civil law perspective?

Yes, see question 4.5 above.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

The public prosecutor's office and the German customs administration are in charge of investigating and enforcing administrative offences. The particular penalty is assessed by the (district) court.

The principle of individualised sentencing is regulated in section 46 of the German penal code ("*Strafgesetzbuch*") ("*StGB*"). This means that the assessment of penalties is especially based on the individual economic and personal circumstances of the convict, as well as the factual circumstances of the offence. The penalty, expressed in so-called "*Tagessätze*", which means a daily rate over a certain time is subdivided into the amount of the penalty per day and the number of days the convict needs to pay. This means that the particular penalty can be adjusted to the economic circumstances of the convict.

The imposition of fines is regulated in section 17 para. 3 OWiG. The assessment of fines is also based on the individual circumstances of the convict as well as the factual circumstances of the offence.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

In principle, the person or company concerned may appeal against the imposition of a fine. As a consequence, the public prosecutor may decide to grant the appellant's request. Otherwise, the matter is brought before the court.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

The public prosecutor's office, with assistance of the Bundesbank and BAFA, enforces sanctions on a national level; see questions 1.2 and 4.3 above.

Public prosecutor's offices on the level of the German federal states, with assistance from the Bundesbank and BAFA, enforce German national sanctions and export control law. There is no parallel state or local law applicable to sanctions and export control violations.

Only in rare and exceptional cases does the Federal Prosecutor General take over (section 142a GVG) the investigation. This only applies if the investigation reaches such a scale that its existence could disrupt or endanger national security or external security of the foreign relations of the Federal Republic of Germany.

4.14 What is the statute of limitations for Economic Sanctions violations?

The statute of limitations applicable is based on whether the sanctions violation is considered a crime or an administrative offence. Further, the statute of limitations applicable in cases where the sanctions violation is considered a crime depends on the maximum prison term associated with the specific sanctions violation.

In cases where the sanctions violation is a crime, specifically in cases of an intentional violation of an arms embargo, the limitation period is 10 years (section 17 para. 1 AWG, section 78 para. 3 No. 3 StGB). In certain offender-related circumstances (e.g., gang membership), the limitation period is also 10 years (section 17 para. 3 AWG, section 78 para. 3 No. 3 StGB). For reckless violations of arms embargoes and intentional violations of EU Sanctions, the limitation period is five years (section 17 para. 4 AWG, section 78 para. 3 No. 4 StGB).

In cases where the sanctions violation is an administrative offence, e.g., in cases of negligent breach of EU Sanctions, the limitation period is three years (section 19 AWG, section 31 para. 2 No. 1 OWiG).

5 General

5.1 If not outlined above, what additional Economic Sanctions-related measures are proposed or under consideration?

Further and additional EU Sanctions on Belarus are contemplated in light of the ongoing political situation in Belarus and specifically in light of the recent events in Japan concerning a member of the Belarus Olympic Team and the situation at the border of Lithuania.

5.2 Please provide information for how to obtain relevant Economic Sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Official information regarding sanctions in non-EU states is published and frequently updated on a sanctions map provided by the EU Commission and can be accessed at: <https://www.sanctionsmap.eu/#/main>.

The above-mentioned EU law can also be found via the internet. See <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012E%2FTXT> and for the TEU see <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT>.

German law is publicly accessible at <https://www.gesetze-im-internet.de/titelsuche.html>. A list of laws available in English can be accessed at https://www.gesetze-im-internet.de/Teilliste_translations.html (please be aware of the disclaimer under "User-Notice").

The leaflet published by the BAFA is very comprehensive and valuable to those new to this area of law as well as experienced practitioners. This nearly 20-sided document can be downloaded free of charge from https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Allgemeine_Einfuehrung/allgemeine_einfuehrung_node.html.

Further guidance for those new to the area of sanctions law can be found on the sanctions page of the European Union. Here, in a structure comparable to this article, individual questions regarding European sanctions law are answered; see https://eeas.europa.eu/headquarters/headquarters-homepage/423/sanctions-policy_en.

A basic overview of the institutions and the legislative process in the EU can be obtained at https://europa.eu/european-union/about-eu/institutions-bodies_de#rechtsetzung.

For comprehensive current developments and more detailed information, in particular, individual sanctions, see <https://www.gibsondunn.com/2019-year-end-sanctions-update/>; for detailed information on ICPs, see <https://www.gibsondunn.com/new-guidance-on-internal-compliance-programs-what-regulators-on-both-sides-of-atlantic-expect-from-international-business/>.

See <https://www.gibsondunn.com/u-s-eu-and-un-sanctions-navigating-the-divide-for-international-business/> for a comprehensive overview of sanctions law, in particular a deeper insight into U.S. sanctions law is recommended: Adam Smith/Stephanie Connor/Richard Roeder, in *U.S., EU, and UN Sanctions: Navigating the Divide for International Business*, published by Bloomberg Law in 2019. Gibson Dunn's International Trade practice and the lawyers on our global sanctions team can help navigate the complex web of varying obligations and restrictions.

EY Forensic & Integrity Services can help companies with sanctions compliance and investigations along with remediation, see https://www.ey.com/en_gl/forensic-integrity-services.



Michael Walther is a partner in the Munich office of Gibson, Dunn & Crutcher LLP. His expertise has a multidisciplinary and international approach covering sanctions and export control, antitrust and competition, data protection and cybersecurity, as well as white-collar defence and investigations. He successfully advises German and international clients, many of which are active in technology-driven industries, on antitrust and competition law. He is regularly involved in complex transactions concerning acquisitions, joint venture scenarios and other forms of cooperation within the industry. He also regularly handles EU and German data privacy and cybersecurity matters.

Gibson, Dunn & Crutcher LLP
Hofgarten Palais, Marstallstrasse 11, 80539 Munich
Germany

Tel: +49 89 189 33 180
Email: mwalther@gibsondunn.com
URL: www.gibsondunn.com



Richard Roeder is a senior associate in the Munich office of Gibson, Dunn & Crutcher LLP. He focuses on international trade compliance and white-collar investigations, as well as transactional regulatory risk assessments, and advises clients from various industries in the areas of sanctions, anti-money-laundering and anti-corruption compliance. In 2018, Mr. Roeder was seconded to Gibson Dunn's Washington, D.C. office where he worked with the U.S. sanctions and export control team and specifically assisted clients in managing the challenges posed by the divergence between U.S. and EU economic and financial sanctions (e.g., regarding the EU Blocking Statute).

Gibson, Dunn & Crutcher LLP
Hofgarten Palais, Marstallstrasse 11, 80539 Munich
Germany

Tel: +49 89 189 33 115
Email: rroeder@gibsondunn.com
URL: www.gibsondunn.com



Meribeth Banaschik is a partner in EY's Forensics & Integrity Services team. As an American litigator and Solicitor of England & Wales with more than 15 years of professional experience, including 10 years' experience in Germany, Meribeth is focused on analytics and applied technologies to isolate and address various risks facing modern global organisations, particularly legal risks. She focuses on the measurement and quality imperatives that impact defensibility and acceptance of technology and technology-driven results in a legal/investigative context. In addition to leading the German eDiscovery and Managed Document Review practice, she is also responsible within Forensics for GDPR compliance projects, document intelligence and litigation operations.

EY Forensic & Integrity Services
Börsenplatz 1, Köln 50667
Germany

Tel: +49 160 939 14325
Email: meribeth.banaschik@de.ey.com
URL: www.ey.com



Bisman Sethi is a Director in EY's Forensic and Integrity Services team. As a Certified Fraud Examiner, with specialisation in Information Technology, Bisman focusses on evaluation and implementation of new technologies, with application of artificial intelligence (AI) in the field of AML and in Combating the Financing of Terrorism (CFT). She has assisted leading financial services organisations examine, assess and automate (using Intelligent Robotics Process Automation (RPA), their compliance processes for transformation and operational optimisation objectives. In addition, she also leads the Screening as a Service (SaaS) ecosystem and works back across the EU region in extending the API led, subscription services programme for sanctions, pep and adverse news for real time compliance monitoring requirements.

EY Forensic & Integrity Services
The Ruby, Dadar West, Mumbai
India

Tel: +91 9619001184
Email: bisman.sethi@in.ey.com
URL: www.ey.com

Gibson, Dunn & Crutcher LLP is a full-service global law firm, with more than 1,400 lawyers in 20 offices worldwide. We are recognised for excellent legal service, and our lawyers routinely represent clients in some of the most complex and high-profile matters in the world. We consistently rank among the top law firms in the world in published league tables. Our clients include most of the Fortune 100 companies and nearly half of the Fortune 500 companies.

www.gibsondunn.com

GIBSON DUNN

EY is one of the world's largest accounting and advisory organisations. Our 300,000 employees in more than 700+ offices in over 150 countries offer comprehensive professional expertise with globally uniform quality standards, helping digital pioneers fight data piracy; guide governments through cash-flow crises; unlock new medical treatments with data analytics; and pursue high quality audits to build trust in financial markets and business – working with entrepreneurs, companies, and entire countries to solve their most pressing challenges.

www.ey.com



Italy

Delfino e Associati Willkie Farr & Gallagher LLP



Gianluca Cattani



Fabio Cozzi

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

The Italian sanction regime is defined by Italy's membership of the European Union ("EU") and basically implements the economic sanctions imposed on countries and non-state entities by the United Nations ("UN") and the EU itself.

The UN imposes sanctions by way of Resolutions. UN sanctions adopted by the UN Security Council under Chapter VII of the UN Charter are implemented by the EU on behalf of EU Member States, including Italy.

The EU is itself a source of "autonomous" (*i.e.* in the absence of any overriding UN Resolution) economic and financial sanctions. At the EU level, sanctions are issued in the context of its Common Foreign and Security Policy ("CFSP"). CFSP Decisions are implemented through EU Regulations – directly applicable in all EU Member States – adopted under Article 215 of the Treaty on the Functioning of the European Union ("TFEU").

Pending the adoption of UN sanctions, Italy may autonomously adopt asset freeze and fund blocking measures against individuals, groups or entities to prevent the financing of terrorism, mass destruction weapon proliferation programmes or any conduct threatening peace and international security. Such measures ("national lists") can be adopted under Article 4-*bis* of Legislative Decree no. 109 of June 22, 2007 and subsequent amendments ("Decree 109/2007") and shall anyway comply with both the obligations set by UN Resolutions and the EU-specific restrictive measures pursuant to Article 215 TFEU.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

While the adoption of sanctions occurs at the EU level, Member States are required to enact and implement adequate and proportionate penalties for sanctions violations.

In Italy, the Ministry of Foreign Affairs and International Cooperation (*Ministero degli Affari Esteri e della Cooperazione Internazionale* – "MAECI") and, in particular, Office I of the Directorate-General for Global Affairs (*Direzione Generale per la mondializzazione e le questioni globali* – "DGMO") is the Italian focal point on sanctions. The MAECI takes part in the European and international negotiations on sanctions and is also responsible for the control of export, transfer and transit of products listed in the EU restrictive measures. In particular, the Unit for the Authorizations of Armament Materials (*Unità per le autorizzazioni dei materiali di armament* – "UAMA") issues the authorisations

for the export, transfer, intermediation and technical assistance related to dual-use items and military items, as well as the authorisations related to anti-torture items and goods listed under EU restrictive measures.

As for asset freezing measures, the Financial Security Committee (*Comitato di Sicurezza Finanziaria* – "CSF"), established within the Ministry of Economic and Finance (*Ministero dell'Economia e delle Finanze* – "MEF"), is responsible for (i) preventing any terrorist organisations from using the Italian financial system, and (ii) implementing asset freezes imposed by the UN, the EU or the MEF, while the Financial Intelligence Unit (*Unità di Informazione Finanziaria* – "UIF"), established within the Bank of Italy, is in charge of collecting financial data and information regarding the listed subject, reviewing and analysing any suspicious transactions and publishing the relevant information.

In relation to the implementation of UN sanctions, pending the adoption of relevant measures by the EU, the Italian authority responsible for implementing the asset freeze measures provided for in Decree 109/2007 is the MEF, upon proposal of the CSF.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

On December 7, 2020, the EU Council adopted the EU Global Human Rights Sanctions Regime, targeting individuals, entities and bodies responsible for, involved in, or associated with serious human rights violations and abuses worldwide. It applies to acts such as genocide, crimes against humanity, other serious human rights violations or abuses. The restrictive measures consist of travel bans, freezing of funds and prohibition to make funds available to listed subjects, directly or indirectly.

Moreover, the EU Parliament and the EU Council approved Regulation 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. The Regulation will enter into force on September 9, 2021, replacing Regulation (EC) 428/2009 and must be implemented across EU Member States, including Italy.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

As for UN sanctions, these sanctions are adopted by the Security Council, pursuant to Article 41 of the UN Charter. As for EU sanctions, these sanctions are issued by the EU Council, by the

adoption of Council Decisions, within the EU CFSP (see question 1.1 above). Italy fully adheres to sanctions imposed at both UN and EU levels.

Pending the adoption of UN Resolutions at the EU level, Italy may autonomously adopt asset freeze and fund blocking measures under Article 4-*bis* of Decree 109/2007 (see question 1.1 above).

In terms of implementation of UN/EU sanctions, Decree 109/2007 provides the framework for implementing measures against the financing of terrorism and activities threatening peace and international security, while Legislative Decree no. 221 of December 15, 2017 (“Decree 221/2017”) provides the framework for implementing trade embargoes and the rules for the export of dual-use items and items suitable to be used for torture or the death penalty.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes, the EU implements UN Resolutions on behalf of its Member States (see question 1.1 above).

Pending the adoption of EU measures, UN sanctions are implemented in Italy under Article 4 of Decree 109/2007: the MEF, acting upon the proposal of the CSF, shall freeze, by ministerial decree, funds and economic resources held, directly or through a third party, by entities or subjects designated by the UN Security Council, according to the criteria established in the UN Resolutions. Such ministerial decrees shall remain in force for six months, unless otherwise established in the decree itself, and cease to have effect once the relevant deliberations by EU institutions are published in the Official Journal of the EU (*i.e.* once the EU specific measures come into effect).

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

Yes, Italy is a Member State of the EU and implements EU sanctions (see questions 1.1 and 2.1 above).

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

The lists of sanctioned individuals and entities are maintained at the EU level. The relevant EU Regulations provide for lists of designated individuals and entities subject to restrictive measures. The EU Council, upon proposal of the High Representatives of the Union for Foreign Affairs and Security Policy, decides whether to include individuals/entities in relevant lists. Persons and entities subject to an asset freeze or travel restrictions are notified of the measures individually by letter, or by means of a notice published by the Council in the C Series of the Official Journal of the European Union.

As for Italy, under Decree 109/2007, the CSF may propose to both UN and EU authorities individuals/entities to include in the lists, keeping into consideration: (i) factual elements that show relations with individuals or entities in connection with, or participation in, terroristic activities; (ii) criminal proceedings

or judicial orders against that person/entity; (iii) elements that can identify the individual/entity to be included in the list; (iv) eventual relationships of the subject with listed entities/individuals; (v) adoption of other measures against the individual/entity; and (vi) any other available information.

In addition, pending the designation by the UN or the EU, the MEF may autonomously adopt measures (the “national lists”, see question 1.1 above).

Either on its own initiative, or upon request of the listed subject, entity or individual, the CSF, through the MAECI, may submit to the Sanctions Committee of the UN or to the EU Council a proposal to remove the listed subject, entity or individual from the related lists.

In case of national lists, either on its own initiative, or upon request of the listed subject, the CSF submits the related request to the MEF.

In order to submit such proposal to the competent international authorities or to the MEF, the Committee shall consider the outcome of the criminal proceedings (if any), as well as any other element indicating the absence of any involvement of the subject in activities related to terrorism or threatening international peace and security.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Listed persons and entities may submit a request to the EU Council together with supporting documentation, requesting that the decision to list them is reconsidered. Moreover, pursuant to the principles affirmed in the EU Charter of Fundamental Rights and the relevant provisions of the EU Treaties, sanctioned individuals and entities have the right to challenge their designation before EU Member State courts.

Finally, listed entities and individuals also have the possibility of challenging the Council Decision before the General Court of the EU, pursuant to Articles 275 and 263 of the TFEU.

As for Italy, the CSF, upon its own initiative or upon request of the listed subject, or within the relevant international or European procedures, submits to the UN Sanctions Committee and to the EU Council proposals for the removal from international and EU lists. In case of national lists, the relevant request is submitted by the CSF to the MEF.

2.6 How does the public access those lists?

As for the EU lists, they are included as annexes to the relevant Decisions and Regulations, and therefore can be accessed on the EU website (<https://eur-lex.europa.eu/>).

However, in order to facilitate the application of financial sanctions, an EU consolidated list of persons, groups and entities subject to CFSP-related financial sanctions has been made available (https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions). Whilst the list is based on the relevant data of the officially adopted texts published in the Official Journal of the EU, the consolidated list is made only to support financial institutions; therefore only the information published in the Official Journal of the EU is deemed authentic.

As for UN sanctions, the UN Security Council publishes a consolidated list, including all individuals and entities subject to measures adopted by the Security Council (<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>).

In Italy, the UIF (<https://uif.bancaditalia.it/adempimenti-operatori/contrasto/index.html>) publishes the links of the EU/

UN lists of designated subjects, as well as those issued by other institutions such as the US Office of Foreign Asset Controls (“OFAC”).

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Italy follows the sanctions regimes imposed at the UN/EU level (which are generally targeted); however, it does not maintain autonomous comprehensive sanctions regimes. The countries subject to sanctions regimes can be found by accessing the EU Sanctions Map (<https://www.sanctionsmap.eu/#/main>).

2.8 Does your jurisdiction maintain any other sanctions?

No, Italy does not maintain other sanctions in addition to those established at the UN and EU level.

2.9 What is the process for lifting sanctions?

Sanctions are meant to be temporary and precautionary measures, and this temporary nature implies that they should be regularly reviewed and amended, lifted or upheld as appropriate. EU Council Decisions imposing restrictive measures provide for specific expiration dates or “sunset clauses”: once the period has expired, the related restrictive measures will cease to have effect unless the EU Council extends the period of application. Once the Decision ceases to have effect, the related Regulation will also cease to have effect in all Member States.

As for the approval of EU restrictive measures, the Council by unanimous decision may lift sanctions, since no parliamentary approval – either by the European Parliament or by national assemblies – is required.

Restrictive measures adopted in the implementation of UN Security Council Resolutions do not have an end date. They are amended or lifted without delay, following a decision by the UN to that effect.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Italy maintains a specific export control regime on dual-use items (Decree 221/2017), as well as on military items (Law no. 185 of July 9, 1990, “Law 185/1990”). Such regime will be amended to implement the recently introduced EU Regulation 821/2021 of May 20, 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast).

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions’ sanctions or embargoes?

Yes, the EU adopted Regulation 96/2271 (the “Blocking Statute”) to protect EU operators, individuals or companies from the extra-territorial application of third country laws listed in its annex (including certain US sanctions targeting Cuba and Iran). The Blocking Statute is also directly applicable in Italy, which has introduced administrative penalties for its violation, from a minimum of EUR 7,746 to a maximum of EUR 92,962.

Pursuant to the Blocking Statute, EU operators are prohibited from complying with the listed foreign laws, unless they are exceptionally authorised to do so by the EU Commission. EU operators whose economic and financial interests are affected by the extra-territorial application of those laws shall inform the EU Commission. Moreover, the Blocking Statute nullifies the effect in the EU of any foreign court ruling based on the foreign laws listed in its annex, and it allows EU operators to recover in court damages caused by the extra-territorial application of the listed foreign laws.

On May 5, 2021, Advocate General Hogan has issued his Opinion in the first case before the Court of Justice of the European Union on the interpretation of Article 5.1 of the Blocking Statute (<https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-05/cp210078en.pdf>).

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as “secondary sanctions”)?

No, the Italian sanction regime does not provide for “secondary sanctions”, which are, conversely, rejected at the EU level.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction’s sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

As a general rule, EU restrictive measures apply in all situations where links exist with the EU. In particular, the standard clause of EU Regulations provides that the restrictive measures apply: (a) within the territory of the Union, including its airspace; (b) on board any aircraft or vessel under the jurisdiction of a Member State; (c) to any person inside or outside the territory of the Union who is a national of a Member State; (d) to any legal person, entity or body, inside or outside the territory of the Union, which is incorporated or constituted under the law of a Member State; and (e) to any legal person, entity or body in respect of any business done in whole or in part within the Union.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Yes, all those who are subject to the EU jurisdiction shall fully comply with the adopted measures and, as such, also to the freezing of assets of listed entities and individuals according to applicable EU Regulations or Italian laws.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes, EU Regulations include provisions on the request of authorisations to use frozen funds and economic resources by listed individuals/entities, as well as on the request of authorisations to export, import or transfer listed goods or to conduct otherwise prohibited activities. The relevant authorisation is granted by the competent Member State authority.

As for Italy, with regard to export control, Decree 221/2017 provides for the issuance of (i) specific individual authorisations, (ii) global individual authorisations, (iii) EU general authorisations, and (iv) national general authorisations. Such authorisations are granted by UAMA, which shall complete the procedure within 180 days from the receipt of the relevant request.

With regard to asset freezes, Decree 109/2007 provides for the procedure to obtain the exemption from the freezing of assets and economic resources. The CSF is responsible for granting the related exemption.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Yes, institutions and entities subject to anti-money laundering obligations (e.g. banking and financial intermediaries and operators, professionals such as accountants, auditors, lawyers and notaries, certain non-financial operators, gambling services providers) communicate to UIF the adopted asset freeze measures, together with the amount and nature of frozen funds and economic resources. The communication must be made within 30 days of the entry into force of the relevant EU Regulations or UN Resolutions, or from the date of possession of funds by the listed subject.

In addition, the same institutions and entities shall promptly communicate to UIF any other available information related to sanctions targets and report suspicious transactions involving individuals or entities listed under counter terrorism and counter proliferation programmes. With regard to measures involving economic resources, the same communications shall be made to the Financial Police.

The EU Regulations providing for financial sanctions require EU economic operators to immediately supply any information which would facilitate compliance with EU sanctions, including details of accounts and amounts frozen, to the competent authorities of the Member State where they are resident or located, and to promptly transmit such information, directly or through the relevant Member State, to the Commission. They must also cooperate with the competent authorities in any verification of such information. Moreover, an economic operator who is aware that a non-listed legal person or entity is owned or controlled by a listed person or entity should inform the competent authority of the relevant Member State and the Commission either directly or through the Member State. Such reporting obligations apply without prejudice to the applicable rules concerning reporting, confidentiality and professional secrecy.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

Any corporation is encouraged (i) to assess the concrete risks of violating sanctions rules associated to its operations, and (ii) to adopt adequate compliance programmes. More specifically, with respect to banks and banks and financial institutions, according to the provisions issued by the Bank of Italy and directed to those entities subject to anti-money laundering obligations, financial institutions and operators shall apply risk-based policies in order to define the degree and extension of client verification (“know your customer” checks) and to implement appropriate procedures and policies. The Bank of Italy expressly requires that client verification shall include whether

the client is listed in any of the lists of designated entities and persons adopted by the EU/UN.

As to the export of dual-use items, the EU Commission Recommendation (EU) 2019/1318 provides non-binding guidance to help exporters identify, manage and mitigate risks associated with dual-use trade controls.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Sanctions violations may imply criminal liability where the Prosecutor finds that the relevant conduct is in breach of specific provisions of the Italian Criminal Code. In particular, providing financial resources to terrorists or terrorist organisations may imply criminal liability with a penalty of up to 15 years’ imprisonment, regardless of the fact that those resources were used for terroristic acts, for individuals, and a penalty of up to EUR 1,549,370 for legal entities. Criminal penalties are also provided under Decree 221/2017 in relation to the export of goods in violation of trade restrictions.

As for dual-use items and instruments of torture, exporting such items or providing services of intermediation in connection thereto, without the required authorisation or with an authorisation obtained by fraudulent means, is punishable by two to six years’ imprisonment or a fine of EUR 25,000 up to EUR 250,000. If the above-mentioned activities are committed in violation of what was provided for by the obtained authorisation, imprisonment of one year up to four years or a fine of EUR 15,000 up to EUR 150,000 applies. Also, refusing to provide information to the competent authority is punishable by up to two years’ imprisonment or a fine of EUR 15,000 up to EUR 90,000.

As to items listed under EU Regulations, violating the prohibition to export listed goods, and/or providing intermediation services or technical assistance in connection with the exportation, is punishable by two to six years’ imprisonment. Exporting goods whose exportation requires an authorisation under EU legal instruments, without obtaining the authorisation or with an authorisation obtained by fraudulent means, is punishable by two to six years’ imprisonment or a fine of EUR 25,000 up to EUR 250,000. Finally, exporting goods in violation of the terms set in the authorisation is punishable by one to four years’ imprisonment or a fine of EUR 15,000 up to EUR 150,000.

As to military items, Law 185/1990 provides that any person who carries out exports, intra-EU transfers, transfers of software and technology relating to military items in breach of the requirements provided for in the authorisation, is punishable by up to five years’ imprisonment or by a fine of between two- and five-tenths of the value of the relevant contract, unless the fact constitutes a more serious criminal offence. Any transaction conducted without the required authorisation is punishable by three to 12 years’ imprisonment or with a fine of between EUR 25,822 and EUR 258,228, unless such fact constitutes a more serious criminal offence.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The Italian Public Prosecutor is responsible for prosecuting offences of a criminal nature. In the case of sanctions/export restrictions violations, the Prosecutor shall immediately notify the MAECI in order for it to adopt any administrative measures

deemed appropriate. In case of offences regulated by Law 185/1990, such notification shall also be made to the Ministry of Defence.

The MAECI together with the Financial Police and the Customs and Monopolies Agency (the “Customs”) are also provided for with inspective powers (for instance, requests of documentation or inspections at the seat of exporter, broker or technical assistance provider) in relation to activities which are prohibited or otherwise restricted by EU Regulations.

4.3 Is there both corporate and personal criminal liability?

No, criminal liability under Decree 221/2017 and Law 185/1990 is provided only for individuals. However, applicable rules on criminal corporate liability (Law Decree no. 231/2001) include criminal offences for terroristic purposes as offences entailing criminal corporate liability.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

See question 4.1 above.

4.5 Are there other potential consequences from a criminal law perspective?

Yes, in the cases under question 4.1 above, the Court orders the seizure of the goods which were used or intended to be used in order to commit the violations. Where the seizure of these goods is not possible, the Court orders the seizure of assets for a value corresponding to the price or profit of the criminal offence. Moreover, criminal liability may also apply to those who facilitate the crimes under question 4.1 above.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

Yes, Decree 109/2007 sets administrative fines for the violation of the restrictive measures adopted against the financing of terrorism and the countries threatening international peace and security. In particular, unless criminal penalties apply, violating the prohibition of using/disposing of frozen assets or of making, directly or indirectly, funds/resources available to designated persons is punishable by a fine of EUR 5,000 up to EUR 500,000. The same fine applies in case of a deliberate participation to activities whose aim is to circumvent, directly or indirectly, an assets freeze. In addition, violating the duties of reporting on the freezing of assets in compliance with the financial measures is punishable by a fine of EUR 500 up to EUR 25,000. Finally, unless the fact constitutes a criminal offence, any other violations of EU Regulations imposing restrictive measures or economic sanctions or the violation of the reporting duty/request of authorisations by Member States is punishable by a fine of EUR 5,000 up to EUR 500,000.

The above administrative fines can be increased up to three times for serious, repeated and/or systematic violations.

Decree 109/2007 – in connection with Law no. 689/1981 – also provides that in the case the above-mentioned violations are committed by a director/employee of a legal entity, both the individual and the entity are severally liable, even where those who materially committed the violation are not unequivocally identifiable.

Law 185/1990 also provides for administrative fines, unless the conduct amounts to a criminal offence, for the violation of the obligations related to the export of military items. The maximum administrative fine amounts to EUR 20,000 (criminal fines may also apply, see question 4.1 above).

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

Supervisory authorities (e.g. the Bank of Italy; Consob, the supervisory authority for the Italian financial products market; IVASS – Institute for the Supervision of Insurance Companies, UIF, the Financial Police and Customs), within their respective areas of competence, are in charge of investigating violations of restrictive measures and trigger the relevant sanctioning proceedings. Any authority having notice of a sanctions violation shall inform the Public Prosecutor (“PM”), the MAECI and the MEF for the relevant investigations and sanctioning proceedings.

As for financial restrictive measures, the Special Department of the Financial Police (*Nucleo speciale di polizia valutaria della Guardia di Finanza*), together with the Financial Police itself, has the power to conduct inspections in order to acquire data and information.

4.8 Is there both corporate and personal civil liability?

Yes, civil/administrative liability applies to both individuals and entities.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

See question 4.6 above.

4.10 Are there other potential consequences from a civil law perspective?

Yes, there may also be additional collateral consequences of a sanctions violation. Decree 109/2007 provides that in case of reiterated (i) violations of the prohibition of using/disposing of frozen assets or making, directly or indirectly, funds/resources available to designated persons, (ii) violations of the duties of reporting on the freezing of assets, or (iii) any other violations of EU Regulations imposing restrictive measures or economic sanctions, the decree imposing penalties for the violation is published – for five years – on the website of the MEF or of the competent authority, indicating the name of those who committed the violation and the legal proceedings in connection thereto. Additional penalties set forth under anti-money laundering regulations may apply (e.g. suspension of the business activity; publication of a statement mentioning the violation and who committed it; and restrictions from managerial positions).

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

In case of violations of restrictive measures, the competent authority (e.g., supervisory authorities, UIF, the Financial Police

or Customs, within their respective areas of competence) serve the defendant (and those who are severally liable for the administrative fine) with a notice of charge. The notice of charge shall be served immediately, or within 90 days if the infringer resides in Italy, or within 360 days if the infringer resides abroad.

The notice of charge shall be transmitted to MAECI – the focal point for economic sanctions and export restrictions – and to MEF, which has competence in case of violations of the financial restrictive measures under Decree 109/2007. The defendant can submit defensive briefs and documents and requests to be heard.

The sanctioning proceedings shall be completed within two years from the date when the MAECI/MEF received the complaint contesting the violation.

The penalties are determined taking into account any circumstance, and, in particular, the value of the transaction, the duration and seriousness of the violation, the degree of liability and the financial capacity of the individual or the legal entity, the advantage obtained/the disadvantage avoided through the violation, the damages caused to third parties, the degree of cooperation with the competent authorities and the existence of previous violations.

The decree imposing administrative fines is not public. In case of reiterated violations of financial restrictive measures, the additional penalty of the publication (for five years) of the sanctioning decree may apply.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

The decree imposing administrative fines can be challenged before the civil Court of Rome, which has exclusive jurisdiction.

According to UIF Annual Report, in 2020, no proceedings for violation of the duty to freeze assets and economic resources were initiated.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Both criminal and civil enforcement take place at the national level only.

4.14 What is the statute of limitations for economic sanctions violations?

As for criminal offences, the statute of limitations is equal to

the maximum penalty provided for the relevant offence and is, however, not less than six years, starting from the date of the violation. In case the statute of limitations is interrupted, it starts running again from the day of the interruption. Also, in case of interruption, the statute of limitation cannot be increased by more than ¼.

As for administrative violations, the statute of limitations is five years from the date of the violation.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

No other additional economic sanctions-related measures are proposed or under consideration in Italy.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

The website of the MAECI (also available in English) provides information on the restrictive measures adopted within the CFSP and is currently in force, as well as a list of all countries, individuals, groups and bodies on which such restrictions apply (https://www.esteri.it/mae/it/politica_estera/politica_europea/misure_deroghe).

The CSF published a set of guidelines on freezing procedures (http://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/linee_guida_CSF.pdf) and a list of the countries currently subject to international financial sanctions (http://www.dt.mef.gov.it/it/attivita_istituzionali/prevenzione_reati_finanziari/embarghi_finanziari/).

The UAMA provides the information necessary to obtain the export authorisations (<https://www.esteri.it/mae/it/ministero/struttura/uama/legislazione.html>).

The EU Sanctions Map (<https://www.sanctionsmap.eu/#/>) provides detailed information on sanctions adopted by the EU Council.

Also, the websites of the EU Council (<https://www.consilium.europa.eu/en/european-council/>) and the EU Commission (https://ec.europa.eu/info/index_en) and of the CFSP (https://eeas.europa.eu/topics/common-foreign-security-policy-cfsp_en) provide detailed information on EU restrictive measures.



Gianluca Cattani is a Partner leading the Corporate and Compliance Department of the Rome office and head of the Italian office's Compliance Practice Group. He has extensive experience in corporate law, M&A, international contracts as well as compliance matters.

In his practice, he has accrued national and international experience in M&A transactions, as well as in corporate law and compliance works for major multinational corporations. His compliance skills also include extensive knowledge of specific related regulatory areas, including data protection, anti-corruption, export control and transactions in countries subject to sanctions or restrictions.

He is appointed as an arbitrator in corporate and contractual disputes and has extensive experience in litigating corporate and compliance cases. He has worked in the UK, USA and Italy where he is also admitted to practise before the Supreme Court.

Delfino e Associati Willkie Farr & Gallagher LLP
Via di Ripetta, 142
00186 Rome
Italy

Tel: +39 06 68636 1
Email: gcattani@delfinowillkie.com
URL: www.willkie.com



Fabio Cozzi (Ph.D.) is a Partner in the litigation practice of the Milan office. He assists multinational companies and financial institutions in connection with domestic and international arbitration proceedings and court litigation, and he regularly advises on compliance issues and investigations related to financial crime, international sanctions and trade restrictions violations.

He previously worked for another major US firm, in Milan and Washington, D.C., assisting clients in connection with arbitration cases and international trade issues. In 2017 he was seconded to the Global Litigation department of one of the largest European banks, working on a major case of violation of international financial sanctions.

Fabio, admitted to practise before the Supreme Court, is ranked by *The Legal 500* (EMEA) 2021 as a Next Generation Partner and has been included among the "rising stars" for commercial arbitration (2020 *Expert Guides*). He has been awarded with the "Rising Star Italy" award in the 2019 Europe Rising Stars Awards in London (*IFLR – Euromoney Legal Awards*).

Delfino e Associati Willkie Farr & Gallagher LLP
Via Michele Barozzi 2
20122 Milan
Italy

Tel: +39 02 76363 1
Email: fcozzi@delfinowillkie.com
URL: www.willkie.com

Willkie Farr & Gallagher LLP is an elite international law firm that provides innovative, integrated legal and business solutions. Willkie's office in Italy was set up in 2000 and operates as Studio Legale Delfino e Associati Willkie Farr & Gallagher LLP. From its inception Studio Legale Delfino e Associati Willkie Farr & Gallagher LLP has consisted of experienced professionals with a well-established practice and clientele and it has rapidly become one of the most important Italian law firms operating in the fields of Dispute Resolution, Compliance, International Trade, Mergers and Acquisitions, Private Equity, Corporate Finance, Corporate Restructuring and Privatisations.

In particular, our Dispute Resolution and Compliance teams are the first port of call for Italian companies seeking strategic representation on issues arising in the US or overseas, where we have in-depth experience dealing with the Department of the Treasury, the Department of Justice and other US authorities. We assist domestic and international clients in complex

internal investigations, criminal and civil law litigation cases deriving from EU/US sanctions and trade restrictions violations, or in connection with white-collar crimes and bribery cases. We regularly support clients in structuring and implementing effective compliance procedures and policies to minimise the risk of financial crime and sanctions violations.

www.willkie.com

**STUDIO LEGALE DELFINO E ASSOCIATI
WILLKIE FARR & GALLAGHER LLP**

Japan

Nishimura & Asahi



Kazuho Nakajima



Masahiro Heike



Yumiko Inaoka

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Japan does not have a comprehensive law authorising sanctions, and instead imposes economic sanctions through various laws and regulations. The primary ground for imposing sanctions is the Foreign Exchange and Foreign Trade Act (“FEFTA”), which mainly regulates cross-border transactions involving goods, services and finances.

The FEFTA authorises the relevant administrative authorities to impose sanctions in any of the following cases:

- (a) the competent minister finds it necessary to fulfil Japan's international obligations under treaties and other international agreements;
- (b) the competent minister finds it necessary as part of Japan's contribution to international efforts to achieve international peace; or
- (c) the Cabinet decides to take countermeasures necessary to maintain peace and security in Japan.

While the majority of Japan's economic sanctions are derived from UN Security Council (“UNSC”) resolutions which fall under the first two categories ((a) or (b) above), Japan also implements sanctions measures based on international cooperation with other countries, such as the U.S. and the EU (category (b) above), as well as unilateral sanctions that are not derived from UNSC resolutions or international cooperation (category (c) above).

The types of transactions that may become subject to sanctions under the FEFTA are (i) import and export of goods (“trade in goods”), (ii) service transactions (such as intermediaries of trade between foreign countries, and transfer of technology and software) (“service transactions”), (iii) payments from Japan to a foreign state and payments between residents and non-residents (“international payments”) (for the definitions of residents and non-residents, please see question 3.1), and (iv) capital transactions (such as contracts for money deposits, trust, money lending, and trading securities) (“capital transaction”). In the following section, the types of transactions falling under (i) and (ii) above are collectively referred to as “international trade” and the types of transactions falling under (iii) and (iv) above are collectively referred to as “financial transactions”.

While the FEFTA is the primary grounds for imposing sanctions, Japan relies on other laws and regulations to impose sanctions when

the FEFTA does not provide the grounds to do so. For example, since the FEFTA does not fully control domestic transactions, the Financial Action Task Force (“FATF”) called upon Japan to enact legislation in 2014 in that regard. Japan responded to the FATF recommendations with the following legislation:

- (i) Amendment to the Act on Punishment of Financing for Offences of Public Intimidation (the “Criminal Financing Punishment Law”) to expand the scope of objects contributing to or used for terrorism that a person may not intentionally provide, from “funds” to “funds and other benefits”, which is interpreted to include goods, houses, information, etc.
- (ii) Enactment of the Act on Special Measures Concerning Asset Freezing, etc., of International Terrorists Conducted by Japan Taking into Consideration United Nations Security Council Resolution 1267, etc. (“Act on International Terrorist Assets-Freezing”), which restricts almost all transactions (including domestic ones) with terrorists listed by the UNSC or the Japanese government.

As Japan's sanctions are primarily governed by the FEFTA, unless specifically mentioned otherwise, the following section will generally cover sanctions on international trade and financial transactions regulated by the FEFTA.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

Under the FEFTA, the competent government agency differs depending on the types of transaction subject to sanctions:

- (a) trade in goods: the Minister of Economy, Trade, and Industry (“METI”);
- (b) service transactions: the Minister of Finance (“MOF”) or METI, depending on the type of service transaction;
- (c) international payments: the MOF or METI, depending on the type of transaction; and
- (d) capital transactions: the MOF or METI, depending on the type of capital transaction.

As a general rule, the METI administers transactions related to the import and export of goods, while the MOF administers transactions related to finance.

The implementation of the Act on International Terrorist Assets-Freezing is implemented by the local Public Safety Commissions. The competent authority for the Criminal Financing Punishment Law is the Ministry of Justice.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

No. The periodical updates on the list of sanctioned individuals and entities and the list of international terrorists were made as explained under question 2.6, but there have been no significant changes or developments impacting the Japanese jurisdiction's sanctions regime over the past 12 months.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The FEFTA authorises the two competent ministers, the MOF and the METI, to impose sanctions if:

- (a) he or she finds it necessary to fulfil Japan's international obligations under treaties and other international agreements; or
- (b) he/she finds it necessary as part of Japan's contribution to international efforts to achieve international peace.

As a general rule, the METI administers transactions related to the import and export of goods while the MOF administers transactions related to finance.

The FEFTA also authorises the Cabinet to impose sanctions if it decides to take countermeasures necessary in order to maintain peace and security in Japan. Such Cabinet decisions must be approved by the Diet. The details of sanctions are determined by the competent ministers mentioned above.

With regard to service transactions, international payments, and capital transactions subject to sanctions, the competent ministers mentioned above authorise the Minister of Foreign Affairs ("MOFA") to designate the individuals and entities with which a person is prohibited from engaging in transactions.

In addition, the Act on International Terrorist Assets-Freezing: (i) requires the National Public Safety Commission to designate individuals and entities that are listed as international terrorists in UNSC resolutions; and (ii) authorises the National Public Safety Commission to designate individuals and entities that it considers as international terrorists, pursuant to UNSC resolution 1373.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes, Japan implements economic sanctions pursuant to UNSC resolutions, as described in question 1.1 above. UNSC resolutions are implemented primarily through the FEFTA and the Act on International Terrorist Assets-Freezing.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

No. However, as described in question 1.1 above, Japan implements sanctions when it finds that their imposition is necessary to contribute to international efforts toward achieving international peace. This type of sanction would be implemented based on international cooperation with other countries, such as the U.S. and the EU. For example, Japan is currently implementing this type of sanction in relation to North Korea's nuclear tests and ballistic missile launch.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Japan maintains lists of individuals and entities subject to sanctions measures for both international and unilateral sanctions.

As explained in question 2.1 above, whether Japan implements sanctions under the FEFTA is decided by the MOF, METI, or the Cabinet. Pursuant to such decisions, the MOF or METI decides upon the specific sanctions measures to be implemented. Finally, the MOFA, authorised either by the MOF or METI, designates individuals and entities with whom a person is prohibited from engaging in service transactions, international payments, and capital transactions, whose names are placed on the sanctions list and who are subject to the sanctions.

Therefore, in order for individuals and entities to be removed from those sanctions lists, the MOF, METI or the Cabinet must decide that such sanctions are no longer necessary. Pursuant to such decisions, the MOF or METI will decide to lift the sanctions on the listed individuals or entities. The MOFA will then amend the sanctions list to remove the designated individuals and entities.

Also, under the Act on International Terrorist Assets-Freezing, the National Public Safety Commission designates international terrorists. The list provided by the National Public Safety Commission must be amended by the Commission as and when necessary.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

(i) Challenge prior to designation

The FEFTA does not provide a specific mechanism by which individuals or entities can challenge their designation prior to their placement on the sanctions list.

Listed individuals or entities may be able to challenge their addition to the sanctions lists under the Administrative Procedure Act; however, there are no publicly available cases or established interpretations regarding the application of the Act to the designation of individuals or entities on the sanctions lists.

The Administrative Procedure Act provides that prior to "adverse dispositions", an administrative agency shall, in principle, grant individuals or entities: (i) an opportunity for a hearing where the individuals or entities may state their opinions and produce evidentiary documents; or (ii) an opportunity for explanation where the individuals or entities in question may submit an explanation of their views on the subject in writing. "Adverse dispositions" means a disposition whereby administrative agencies directly impose duties upon specified persons or limit their rights. Prior to the designation, an individual or entity may be entitled to the procedures described above.

On the other hand, the Act on International Terrorist Assets-Freezing clearly requires the National Public Safety Commission to hold a hearing prior to the designation unless the Commission believes the hearing will make it extremely difficult to enforce sanctions.

(ii) Challenge after designation

Neither the FEFTA nor the Act on International Terrorist Assets-Freezing provides a specific mechanism by which individuals or entities can challenge their designation after their designation on the sanctions list.

However, an individual or entity may be able to either: (i) request an administrative review by the original or higher

administrative agencies regarding the dispositions, under the Administrative Complaint Review Act; or (ii) bring an action in court for revocation of the original administrative disposition, under the Administrative Case Litigation Act. It should be noted that there are no publicly available cases or established interpretations regarding the application of these Acts to the designation of individuals or entities on the sanctions lists.

2.6 How does the public access those lists?

The consolidated list of sanctioned individuals and entities designated pursuant to the FEFTA can be found on the website of the MOF and is available at the following URL (in Japanese only) (last accessed 3 June 2021): http://www.mof.go.jp/international_policy/gaitame_kawase/gaitame/economic_sanctions/list.html.

The consolidated list of international terrorists designated by the National Public Safety Commission pursuant to the Act on International Terrorist Assets-Freezing can be found on the website of the National Public Safety Commission and is available at the following URL (in Japanese only) (last accessed 3 June 2021): <https://www.npa.go.jp/bureau/security/terrorism/zaisantouketu.html>.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Japan has unilaterally implemented a general ban on exports to and imports from North Korea, and a ban on embankment of North Korean vessels. In addition, Japan has implemented a general ban on imports from Crimea and Sevastopol.

2.8 Does your jurisdiction maintain any other sanctions?

In addition to the sanctions imposed pursuant to UNSC resolutions or taken in cooperation with other countries, Japan imposes unilateral sanctions when a Cabinet decision is made to take countermeasures that are particularly necessary in order to maintain peace and security in Japan.

Japan has implemented unilateral sanctions measures against North Korea due to rising concerns about its nuclear and missile activities, and also about its involvement in abductions of Japanese citizens. Unilateral sanctions measures against North Korea include a ban on entry into Japan by North Korean nationals and vessels, a ban on all export to and import from North Korea, a ban on payments to individuals and entities with North Korean residency, etc.

2.9 What is the process for lifting sanctions?

As explained in question 2.1 above, whether Japan implements sanctions under the FEFTA is decided by the MOF, METI, or the Cabinet. Pursuant to such decisions, the MOF or METI decides the specific sanctions measures to be implemented, by way of regulations or public notices.

Therefore, in order for a sanction to be lifted (other than the deletion of individuals and entities from the sanctions list, which is determined by the MOFA), the MOF, METI or the Cabinet must decide that sanctions are no longer necessary. Pursuant to such decisions, the MOF or METI must amend the regulations or public notices which determined the specific sanctions measures to be implemented.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes. The Japanese export control regime is also implemented primarily through the FEFTA, which enforces two types of control: list control; and catch-all control. List control requires exporters to apply for a licence when exporting or transferring sensitive military and dual-use items (goods, technology, or software), as designated in accordance with international export control regimes, to a foreign country. Catch-all control requires the same when less sensitive items being exported will be used for certain applications related to weapons of mass destruction (“WMD”) or conventional arms.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions’ sanctions or embargoes?

No, it does not.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as “secondary sanctions”)?

No. However, please see question 3.1 below regarding extraterritorial application of the FEFTA and the Act on International Terrorist Assets-Freezing.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction’s sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

With regard to international payments subject to sanctions, (i) “residents” or “non-residents” who intend to make payments from Japan to a foreign state must obtain permission from competent authorities, and (ii) “residents” who intend to make payments to or receive payments from “non-residents” must also obtain permission, under the FEFTA. “Resident” is defined as: (i) a natural person with a domicile or residence in Japan; or (ii) a corporation with a principal office in Japan, and “non-residents” are defined as a natural person or corporation other than a resident.

Residents or non-residents who intend to conduct capital transactions are required to obtain permission.

However, with regard to service transactions subject to sanctions, only residents are required to obtain approval when the relevant resident intends to conduct service transactions with non-residents.

With regard to trade in goods subject to sanctions, the FEFTA requires exporters from Japan or importers to Japan to apply for approval of the sanctioned trade.

In addition, the FEFTA is applied to actions in a foreign country by the representative, agent, employee, or other worker of (i) a corporation with a principal office in Japan, or (ii) a person with a domicile in Japan if such transactions are undertaken in connection with that corporation’s/person’s assets or business.

The Act on International Terrorist Assets-Freezing restricts almost all transactions in Japan with designated terrorists, regardless of the counterparts’ nationality or residency. In addition, it

is also applied to transactions in foreign countries made by (i) a corporation with a principal office in Japan, or (ii) a natural person with a domicile or address in Japan.

The Criminal Financing Punishment Law criminalises any persons in Japan who provide terrorists and their supporters with funds, services, real estate, goods, information and other benefits. This law is also applied to persons in a foreign country, regardless of nationality, when such acts are also governed by the International Convention for the Suppression of the Financing of Terrorism, even if they are committed outside of Japan.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

No. However, the Act on Prevention of Transfer of Criminal Proceeds (“Criminal Proceeds Act”) requires banks and other financial institutions to confirm the identities of their customers, and to notify the government authorities of “suspicious transactions”. “Suspicious transactions” are transactions of property which is suspected to be criminal proceeds or transactions by a customer, etc. who is suspected to have been conducting acts that constitute specific crimes, including acts of terrorism, as stipulated in the Criminal Financing Punishment Law, and exports/imports that violate economic sanctions under the FEFTA.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

The FEFTA and the Act on International Terrorist Assets-Freezing requires a person to obtain permission or approval for financial transactions and international trade that are subject to economic sanctions. A person may apply for permission or approval to undertake such transactions, but generally speaking such permission will not be granted.

The Act on International Terrorist Assets-Freezing clearly stipulates a list of conditions under which transactions are permitted. For example, payments are permitted when they are used for “expenses usually required for normal living” of the terrorists and their families.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

As explained in question 3.2 above, the Criminal Proceeds Act requires banks and other financial institutions to notify the government authorities of “suspicious transactions”, including transactions suspected to be related to specific crimes, acts of terrorism stipulated in the Criminal Financing Punishment Law, and exports/imports that violate economic sanctions.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

Although the MOF has established compliance guidelines in order for banks and other financial institutions to effectively comply with their obligations under the FEFTA, as stated in question 3.2 above, the FEFTA does not create legally binding compliance standards or programmes with regard to financial transactions.

The Financial Services Agency has also established the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism”, which clarify the required actions and expected actions to be implemented by each financial institution in order to comply with the identification and verification obligations, etc., required in the Criminal Proceeds Act.

With regard to export control, although not specific to sanctions, the FEFTA requires all persons engaged in exports of goods or transfers of technology to establish certain kinds of internal control systems in order to comply with the export control regulations.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

The FEFTA provides for criminal penalties for violating such laws and regulations.

As noted above, in terms of financial transactions and service transactions, the FEFTA requires a person to obtain permission from the competent authorities for transactions that are subject to sanctions. If a person engages in such transactions without such permission, that person will be subject to: (i) imprisonment for not more than three years; or (ii) a fine of not more than one million yen (provided that if three times the value of the subject matter of the violation exceeds one million yen, the fine is not more than three times that value).

Next, in terms of trade in goods, the FEFTA requires a person to obtain approval for certain transactions that are subject to economic sanctions. If a person engages in such transactions without such approval, the person will be subject to: (i) imprisonment for not more than five years; or (ii) a fine of not more than 10 million yen (provided that if five times the value of the subject matter of the violation exceeds 10 million yen, the fine is not more than five times that value).

These penalties are imposed on an individual who violates economic sanctions laws and/or regulations. For the penalties imposed on a corporation, please see question 4.3 below.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The police and public prosecutors investigate and prosecute those offences as criminal cases.

4.3 Is there both corporate and personal criminal liability?

The FEFTA provides for both corporate and personal criminal liability.

With regard to financial transactions and service transactions, if a violation is committed in connection with the business or assets of a corporation, the corporation (in addition to the offender, as explained in question 4.1 above) will be subject to a fine of not more than one million yen (provided that if three times the value of the subject matter of the violation exceeds one million yen, the fine is not more than three times that value).

With regard to trade in goods, if a violation is committed in connection with the business or assets of a corporation, the corporation (in addition to the offender, as explained in question 4.1 above) will be subject to a fine of not more than 500 million yen (or, if five times the value of the subject matter of the violation exceeds 500 million yen, a fine of not more than five times that value).

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

Please see questions 4.1 and 4.3 above.

4.5 Are there other potential consequences from a criminal law perspective?

No. However, the FEFTA endeavours to ensure the effectiveness of economic sanctions by establishing provisions regarding administrative sanctions in addition to criminal penalties.

To be more specific, in terms of financial transactions and service transactions, the FEFTA states that the Minister in charge may prohibit financial transactions and service transactions by the relevant person for a period not exceeding one year (Article 16-2, Article 22, paragraph (1) and Article 25-2, paragraph (4) of the FEFTA).

In addition, in terms of foreign trade, if a transaction for which approval must be obtained is conducted without such approval, the FEFTA states that the METI may prohibit importation or exportation by the relevant person for a period not exceeding one year (or three years in the case of a sanction independently imposed by Japan) (Article 53, paragraph (2) of the FEFTA).

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

The FEFTA does not provide for civil penalties.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

This is not applicable in Japan.

4.8 Is there both corporate and personal civil liability?

This is not applicable in Japan.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

This is not applicable in Japan.

4.10 Are there other potential consequences from a civil law perspective?

This is not applicable in Japan.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

This is not applicable in Japan.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

This is not applicable in Japan.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal enforcement only exists at the national level.

4.14 What is the statute of limitations for economic sanctions violations?

With respect to the criminal penalties provided in the FEFTA for individuals who violated sanctions on financial transactions and service transactions, the statute of limitations is three years. With respect to the criminal penalties for those who violated sanctions on trade in goods, the statute of limitations is five years.

The statute of limitations for corporate criminal liability provided in the FEFTA is three years, regardless of the type of relevant transaction.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

Reflecting the lack of a human rights sanctions regime, there have been calls to introduce such a sanctions regime in Japan. In particular, in April 2021, a parliamentary group called the “Nonpartisan Parliamentary Association for Reconsidering Human Rights Diplomacy” was established to promote the adoption of a sanctions regime focused on human rights violations. As of May 2021, the association has published on its website a brief summary of a draft bill to introduce a new act and amend existing laws, including the FEFTA, that would authorise imposing sanctions in response to grave human rights violations.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Information about the relevant laws, regulations, administrative actions, and guidance relating to economic sanctions, can be obtained from the following websites (in Japanese) (last accessed 3 June 2021):

- Website of the MOF: https://www.mof.go.jp/international_policy/gaitame_kawase/gaitame/economic_sanctions/index.htm.
- Website of the METI: https://www.meti.go.jp/policy/external_economy/trade_control/01_seido/04_seisai/seisai_top.html.
- Website of the Center for Information on Security Trade Control (“CISTEC”): <http://www.cistec.or.jp/export/keizaiseisai/index.html>.

English translations of some of the relevant laws and regulations can be found at the following websites (last accessed 3 June 2021):

- FEFTA: <http://www.japaneselawtranslation.go.jp/law/detail/?id=3267&vm=04&re=01>.
- Criminal Financing Punishment Law: <http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2977&re=01&vm=02>.



Kazuho Nakajima primarily assists corporate clients with mergers and acquisitions, international commercial transactions, regulatory matters, litigation and disputes. Against the background of rising concern over national security, technology competition and counterterrorism in the international community, he engages in transactions relating to U.S. economic sanctions and export control regulations for non-U.S. companies, as well as Japanese export controls and money laundering regulations. He has extensive experience with complex legal issues, such as mergers and acquisitions by a public-private investment fund in the context of a business turnaround, a dispute between a securities company and a stock exchange involving extensive damages, adoption of anti-takeover defence measures for the first time in Japan, expansion of foreign businesses into the Middle East involving geopolitical risks, and a commercial arbitration involving a significant amount of claims regarding price adjustment clauses in a merger and acquisition.

Nishimura & Asahi
Otemon Tower, 1-1-2 Otemachi
Chiyoda-ku, Tokyo 100-8124
Japan

Tel: +81 3 6250 6411
Email: k.nakajima@nishimura.com
URL: www.nishimura.com



Masahiro Heike is a partner of Nishimura & Asahi, where he specialises in international trade law (WTO, FTAs, trade remedies, export controls, etc.) and competition law (anti-monopoly), and frequently advises private companies and government agencies in matters related thereto. Mr. Heike worked in the Ministry of Economy, Trade and Industries of Japan from 2016 to 2018 and has been involved in various international trade disputes.

Nishimura & Asahi
Otemon Tower, 1-1-2 Otemachi
Chiyoda-ku, Tokyo 100-8124
Japan

Tel: +81 3 6250 6566
Email: m.heike@nishimura.com
URL: www.nishimura.com



Yumiko Inaoka is an associate at Nishimura and Asahi. She advises both domestic and international clients on various matters of sanctions law, export control regulations and foreign investment regulations, and has experience in dispute resolution in international trade law. She is also active in competition law matters, especially in cross-border transactions, and has handled merger filings across multiple international jurisdictions.

Nishimura & Asahi
Otemon Tower, 1-1-2 Otemachi
Chiyoda-ku, Tokyo 100-8124
Japan

Tel: +81 3 6250 6566
Email: y.inaoka@nishimura.com
URL: www.nishimura.com

Nishimura & Asahi (N&A) is Japan's largest law firm, covering all aspects of domestic and international business and corporate activity. The firm has over 700 Japanese and foreign lawyers – employing over 1000 support staff, including tax accountants, patent attorneys, senior Japanese and foreign business support professionals, and paralegals. In addition to their experience working in a top global law firm, many members of N&A speak more than one language, possess advanced international law and other degrees, and are licensed in multiple jurisdictions.

N&A's strong professional relationships with other eminent law firms worldwide and its long-standing relationships with prominent corporations in the manufacturing, distribution, and retail industries, further strengthen its ability to service both Japanese and foreign clients at the highest international standards. In addition to this focus on international corporate

and financial transactions, N&A is increasingly involved in advising and assisting clients in communications, information technology, e-commerce, service, and other emerging industries, where it is adept at finding novel legal solutions for the problems faced by these cutting-edge businesses.

www.nishimura.com

**NISHIMURA
& ASAHI**

Korea

Yulchon LLC



Tong-chan Shin



Jae Hyong Woo



Yong Ju Lee

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

In general, the Republic of Korea's sanctions regime consists of (i) regulations related to general international sanctions, namely the Foreign Exchange Transactions Act and the Act on Prohibition against the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (the "Prohibition of Financing Terrorism Act"), and (ii) national export controls governed by the Foreign Trade Act as below.

The **Foreign Exchange Transaction Act** regulates transactions, payments or receipts of funds and other similar acts between Korea and any foreign country. Notably, the Ministry of Economy and Finance ("MOEF"), which enforces the Foreign Exchange Transaction Act, may require any person who intends to make payment from Korea to a foreign country, or residents who intend to make payment to non-residents or to receive payment from non-residents, obtain permission in the interest of enforcing treaties entered into by Korea or contributing to international endeavor for maintaining international peace and security.

The **Prohibition of Financing Terrorism Act** aims to implement the International Convention for the Suppression of the Financing of Terrorism and the United Nations Security Council resolutions. In case the Financial Services Commission ("FSC"), which enforces the Prohibition of Financing Terrorism Act, determines that any act committed by an individual, corporation or organisation is related to the proliferation of weapons of mass destruction, with the consent of the relevant authorities, the FSC may designate such person as "a person subject to restrictions on financial transactions, etc." ("Restricted Person"). Financial institutions and their employees are prohibited from engaging in financial transactions with the Restricted Person. Further, supplying funds or property to benefit any individual, corporation or organisation who intends to engage in an act of terrorism is prohibited.

The **Foreign Trade Act** regulates imports and exports, with an objective to fulfil and further various international treaties and multilateral regimes (Articles 5 and 11). The Ministry of Trade, Industry and Energy ("MOTIE"), which enforces Foreign Trade Act, is responsible for designating and publicly

announcing goods or technologies that require export permission to maintain international peace and security as well as national security.

Transactions with North Korea are subject to a set of special regulations under the Inter-Korean Exchange and Cooperation Act, which is enforced by the Ministry of Unification ("MOU").

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The MOEF, the MOTIE, the MOU, and the FSC are the authorities that administer and enforce Korea's sanction regime. Please refer to questions 1.1 above.

When the FSC adds a person onto the Restricted Person list, it can only do so with the consent of the relevant authorities, namely MOEF, Ministry of Foreign Affairs ("MOFA"), and the Ministry of Justice ("MOJ").

As for export control, the competent authorities are the Commissioner of the Nuclear Safety and Security Commission, the Administrator of the Defense Acquisition Program Administration, and the MOTIE.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

In the past 12-month period, only minor amendments to the sanctions laws have been made. None of such amendments would bring any meaningful change or development to the existing law.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

In addition to the description in question 1.1, the sanctions laws are implemented as follows through the relevant subordinate statutes:

- (1) In principle, there is no restriction on foreign exchange transactions under the Foreign Exchange Transaction Act.

Nevertheless, some exceptional cases may result in such foreign exchange transactions being prohibited or subject to approval. For example, certain foreign exchange transactions could be limited in the interest of promoting and maintaining international peace and security. In connection therewith, the MOEF has published the Guidelines on Payment and Receipt for the Fulfilment of Obligations for International Peace and Security Maintenance, etc. (the “Guidelines”) and, as of August 2020, the sanctions list in Article 2 of the Guidelines is as follows (the “Sanctioned Person”):

(i) Sanctioned by 14 of United Nations Security Council resolutions (“UNSC RES”): 1. UNSC RES 751 in 1992 and RES 1907 in 2009 (re: Somalia and Eritrea); 2. UNSC RES 1267 in 1999, RES 1989 in 2001 and RES 2253 in 2015 (re: ISIL, Al-Qaeda); 3. UNSC RES 1518 in 2003 (re: Hussein government of Iraq); 4. UNSC RES 1521 in 2003 (re: Liberia); 5. UNSC RES 1533 in 2004 (re: DR Congo); 6. UNSC RES 1572 in 2004 (re: Côte d’Ivoire); 7. UNSC RES 1591 in 2005 (re: Sudan); 8. UNSC RES 1718 in 2006 (re: North Korea); 9. UNSC RES 2231 in 2015 (re: Iran); 10. UNSC RES 1970 in 2011 (re: Gaddafi government of Libya); 11. UNSC RES 1988 in 2011 (re: Taliban in Afghanistan); 12. UNSC RES 2127 in 2013 (re: Central African Republic); 13. UNSC RES 2140 in 2014 (re: Yemen); and 14. UNSC RES 2206 in 2015 (re: South Sudan).

(ii) Sanctioned by four US Executive Orders (“EO”): EO 13224 (re: terrorism); EO 13382 (re: weapons of mass destruction); EO 13573 (re: Syria); and EO 13582 (re: Syria).

(iii) Sanctioned by the Council of the European Union. The UNSC RES included under (i) above are self-executing and implemented nationwide. As for US EOs and the European Union sanctions, the MOEF has the authority to determine which of those to implement. The Minister may impose additional sanctions for national security purposes in consultation with the MOFA, the MOJ, the MOTIE, the Commissioner of the FSC and other relevant authorities.

Under Article 3 of the Guidelines, an approval from the Governor of the Bank of Korea is necessary to make a payment to, or receive a payment from, a Sanctioned Person. The foregoing applies to not only residents but also non-residents who are under the jurisdiction of the Foreign Exchange Transactions Act. In cases of a transaction with an individual or organisation in Iran, the foreign exchange bank must confirm relevant matters of such transaction, including the payment and receipt of funds, the port of entry and the relevant carrier (Article 4 of the Guidelines).

(2) In accordance with the Prohibition of Financing Terrorism Act, the FSC designates a Restricted Person and enforces a set of rules concerning such designation called the Regulations on Designation and Cancellation of Restricted Person on Financial Transactions, etc. As of August 2020, a total of 685 targets are included in the sanctions list:

(i) Targets designated by each of the Security Council Committee composed under: (a) UNSC RES 1267 in 1999, UNSC RES 1989 in 2011, and UNSC RES 2253 in 2015; (b) UNSC RES 1718 in 2006; (c) UNSC RES 2231 in 2015; (d) UNSC RES 1988 in 2011 and its following decision or UNSC RES 1267 in 1999, UNSC RES 1989 in 2011 and UNSC RES 2253 in 2015; (e) UNSC RES 1718 in 2016; (f) UNSC RES 2231 in 2015; and (g) UNSC RES 1998 in 2011.

(ii) Targets designated by the FSC in accordance with the below UNSC RES:

(a) UNSC RES 1373 in 2001 (re: the 9/11 terror attack); and

(b) UNSC RES 1718 in 2006 and following decisions (re: North Korea).

The UNSC resolutions in (i) above are self-executing in South Korea without permitting any additional changes in the list; list (ii) above can be revised to add further targets at the FSC’s discretion (e.g. to reflect US EOs, etc.).

Under the Guidelines, any person designated as the Restricted Person must obtain prior permission from the FSC in order to carry out financial transactions with a financial institution (Article 2-a). Where such Restricted Person intends to dispose (such as transfer or donation), transfer possession, or change the original status of movable property, real estate, bonds and other assets or other property rights, the Restricted Person or the counterparty must obtain permission from the FSC (Article 2-b).

(3) The Notice of Import and Export of Strategic Items which is published under the Foreign Trade Act by the Minister of Trade, Industry and Energy implements Korea’s national export controls. Export control with respect to (a) items listed as Strategic Items in the above Regulations (equivalent to EAR 99), and (b) non-Strategic Items are both governed by the Foreign Trade Act. The following authorities are responsible for processing license applications for each type of items:

(i) the MOTIE for dual-use items;

(ii) the Commissioner of Nuclear Safety and Security Commission for nuclear trigger items (item with special purposes in nuclear industry); and

(iii) the Administrator of the Defense Acquisition Program for military items.

Where the Notice of Import and Export of Strategic Items and the Notice of Arms Embargoes overlap, all the restrictive conditions of both notices must be satisfied. Moreover, the Notice of Special Measures on Trade to Fulfil Obligations for International Peace Security Maintenance etc. under the Foreign Trade Act (“Peace Notice”) imposes international arms embargoes. The Kimberley Process on the diamond trade, international embargoes of the United Nations against Central Africa Republic, DR Congo, Iraq, Lebanon, Libya, North Korea, Somalia, Sudan, Syria and Yemen are also regulated by the Peace Notice.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes, the Korean government implements the United Nations sanctions as described above. Please refer to question 2.1.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

No, Korea is not a member of a regional body issuing sanctions.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Yes, the Korean government maintains a list of sanctioned individuals and entities. The lists of Sanctioned Persons and Restricted Persons are managed and announced in accordance with the Foreign Exchange Transaction Act, the Prohibition of Financing Terrorism Act, the Foreign Trade Act and their subordinate statutes (see question 2.1). The lists include:

- (i) those directly implemented from the UN sanctioned persons;
- (ii) those designated and implemented by the MOEF from the UN sanctioned persons, US sanctioned persons and EU sanctioned persons; and
- (iii) those designated and implemented unilaterally by relevant authorities of Korea.

The list of Sanctioned Person under the Foreign Exchange Transaction Act and the Guidelines is managed and announced by MOEF. With the consent of the MOEF, the MOFA and the MOJ, the FSC may add individuals and entities to the Restricted Person list.

Except for the removal challenges described in question 2.5 below, there are no prescribed processes to remove a particular person from the sanctions lists.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Regarding the Restricted Person list, an individual or entity may challenge its addition to a sanctions list in accordance with the procedure laid out in Article 4.7 of the Prohibition of Financing Terrorism Act and the Regulation on the Designation and Cancellation of Restricted Person on Financial Transactions etc. Specifically, raising the challenge can be carried out by requesting the cancellation of the designation to (1) the UNSC or the FSC, (2) the Focal Point of the United Nations, and (3) the Ombudsperson of the United Nations to cancel the designation.

On the other hand, there is no such challenge procedure available for the sanctions lists established under the Foreign Exchange Transaction Act and the Foreign Trade Act. In theory, however, a person may contest its designation against the designated jurisdiction in the following cases: (a) if the designation overlaps with the sanctions list of the Prohibition of Financing Terrorism Act, the complaint procedure described in the above paragraph could be available; or (b) if the designation is found only in the lists of the Foreign Exchange Transaction Act and the Foreign Trade Act without overlap, it may be contested against the designated jurisdiction pursuant to the Administrative Appeals Act and the Administrative Litigation Act.

2.6 How does the public access those lists?

The public can access the lists through the following links which are provided in Korean:

- Sanctioned Person lists are available at the MOEF's website:
 - http://www.moef.go.kr/com/bbs/detailComtPolbbsView.do?menuNo=5020200&searchNttId1=MOSF_000000000005834&searchBbsId1=MOS-FBBS_0000000000039.
 - http://www.moef.go.kr/com/bbs/detailComtPolbbsView.do?menuNo=5020200&searchNttId1=MOSF_000000000006720&searchBbsId1=MOS-FBBS_0000000000039.

- http://www.moef.go.kr/lw/denm/detailTbDenmView.do?searchBbsId1=MOSFBBS_000000000120&searchNttId1=MOSF_00000000011600&menuNo=7030000.

- Restricted Person lists are available at the FSC's website: <https://www.fsc.go.kr/po040200/24762>.
- Denial lists for export controls are available at <https://yestrade.go.kr> (by using the "DENIAL LIST 검색" menu).

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Countries designated by the UNSC are also sanctioned by Korea. The sanctioned countries as of August 2020 are Central Africa Republic, DR Congo, Iraq, Lebanon, Libya, North Korea, Somalia, Sudan, Syria and Yemen. Under the Inter-Korean Exchange and Cooperation Act, any transaction with North Korea, such as exchange of items or trading, requires approval from the MOU.

Sanctions under the Foreign Exchange Transaction Act and the Prohibition of Financing Terrorism Act are limited to the listed entities, and the Peace Notice (see question 2.1) which regulates international arms embargoes is also limited to the trading of certain arms and weapons to 10 sanctioned countries.

As such, not all economic activities are covered under these sanctions, as is in the case of the US sanctions against Iran.

Regarding sanctions against Iran, Korea also had a relatively comprehensive sanctions programme until Iran sanctions were eased by the international community in January 2016 according to the Joint Comprehensive Plan of Action. After the adoption of the UNSC RES 1929 in June 2010, the Korean government introduced a set of regulations governing transactions with Iran, which largely incorporated the relevant US laws and regulations that was in place. The regulations introduced measures to regulate financial transactions with Iranian banks, trade of goods and construction projects relating to Iran's energy sector. While the Korean government did not directly impose any sanction or regulation on private entities doing business with Iran (the Korean regulatory schemes concerning trades and investments were mainly based on industry self-regulations and guidelines issued by various self-regulatory organisations such as Korea International Trade Association and International Contractors Association of Korea), under the Foreign Exchange Transaction Act and the Guidelines, whoever makes payment to or receive payment from Iran had to obtain approval from the Governor of the Bank of Korea, even if the concerned Iranian party was not listed as Sanctioned Person. However, since January 2016 Korean government has eased most of the sanctions related to trade with and investment to Iran and did not re-enforce such regulations even after the US re-imposed sanctions against Iran in August 2018.

However, since the Trump Administration of the US did not give any waivers under the National Defense Authorization Act of Fiscal Year 2012 to any foreign country which has been importing Iranian crude oil including South Korea, from May 2019, South Korea's export to Iran has been stopped, payments of which have been made through the proceeds of the Iranian crude oil by Iran except for the goods with regard to humanitarian purposes.

2.8 Does your jurisdiction maintain any other sanctions?

No, South Korea does not maintain any other sanctions.

2.9 What is the process for lifting sanctions?

The basis of sanctions stipulated in the Foreign Exchange Transaction Act, Prohibition of Financing Terrorism Act, and Foreign Trade Act cannot be lifted without amending the statutes. In order to amend a statute, attendance of a majority of National Assembly's total members, and the concurrent vote of a majority of the members present are required. However, within the limits of the above Acts, the relevant authorities have a wide discretion to lift particular sanctions and remove individuals and entities from the sanctions lists, based on its policies.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Please refer to the Foreign Trade Act as discussed in question 2.1.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

No, it does not.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

No, it does not.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

The parties or transactions subject under the Foreign Exchange Transaction Act are as follows: (1) foreign exchange transaction in Korea; (2) transactions, payments or receipts thereof between Korea and any foreign country (including such acts performed in any foreign country which have an effect in Korea); (3) transactions between an individual or a foreign legal entity which are denominated or payable in Korean currency; and (4) acts conducted by an individual or a legal entity in Korean in connection with his/her assets or business in a foreign country (Article 2.1).

The Prohibition of Financing Terrorism Act applies also to a foreigner who violated provisions of the Act in relation to diplomatic offices or to a foreigner who later falls within the jurisdiction of Korea following his/her violation thereof.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Acts relating to the disposition of assets of the Restricted Person (such as financial transactions, transfer of property, bonds and other property, or property rights and the transfer or changes of assets) are prohibited under the Prohibition of Financing Terrorism Act. These regulations are regarded to have the effects of asset freezing.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

The Foreign Exchange Transaction Act and its related regulations (such as Article 3 of the Guidelines) provides that any payment to, or receipt of funds from, a Sanctioned Person must be approved by the Governor of the Bank of Korea.

Under Article 4.4 of the Prohibition of Financing Terrorism Act, permission from the FSC must be obtained in order to engage in transactions with a Restricted Person.

As for the permit on export controls, please refer to the discussion in question 1.1 regarding the Foreign Trade Act.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Any employee of a financial institution, as soon as he/she become aware of the fact that any assets received from a financial transaction are funds for terrorism or the proliferation of weapons of mass destruction, must report such fact to the relevant investigative authority, notwithstanding the provisions of other Acts or subordinate statutes.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

Companies are not legally required to have in place compliance programmes dedicated for sanctions purposes.

In the context of export control, however, only those companies that have the following implemented can be designated as a company with an internal compliance programme under the Foreign Trade Act:

- (i) capacity to classify the strategic items;
- (ii) capacity to analyse the importers and end users;
- (iii) compliance committee and operational capability (Article 25.1 of the Foreign Trade Act); and
- (iv) compliance regulations, including a representatives' duty to make a declaration on export management, organisation of the autonomous export control body, establishment of a process to classify the strategic items/export examination process, shipping management (or technology transfer management), audits, training, document management, violation reporting and corrective action, information security management, etc. (Article 71 of the Notice of Import and Export of Strategic Items.)

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

For violations of sanctions under the Foreign Exchange Transaction Act, a penalty of up to three years of imprisonment and/or a fine not exceeding either (a) KRW 300 million, or (b) three times the transaction value can be imposed if any person do not obtain the approval from the Governor of the Bank of Korea before making payment to or receiving payment from Sanctioned Person (Articles 27-2, 15).

The Prohibition of Financing Terrorism Act stipulates that the penalty may include (1) imprisonment for up to 10 years or

ines of up to KRW 100 million in case of support for individuals or organisations that intend to engage in an act of terrorism as defined under the law, or (2) imprisonment for up to three years or fines of up to 30 million in the case of:

- (i) a Restricted Person or his/her counterparty who performs an act that requires FSC's permission after obtaining such permission by deception or other fraudulent means;
 - (ii) a Restricted Person who performs an act that requires FSC's permission without obtaining such permission; and
 - (iii) a Counterparty of Restricted Person who performs an act that requires FSC's permission without obtaining such permission (only when counterparty knows that Restricted Person is designated as such), and
- (3) imprisonment for two years or less or a fine of KRW 10 million or less in case of reporting duty violation (Article 6).

The penalty for exporting without the export licences required under The Foreign Trade Act can be up to five times of the price of the relevant transaction or imprisonment up to seven years (Article 53). Negligence is also subject to punishment (Article 56).

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The department in charge of each statute (see question 1.2) may refer any criminal offences to investigation organisation (i.e., police or prosecutors' office). While investigation is left to the prosecution and the police, criminal charges are filed only by the prosecution followed by the court's judgment on the final punishment.

4.3 Is there both corporate and personal criminal liability?

Yes, there is both corporate and personal criminal liability under Article 31 of the Foreign Exchange Transaction Act, Article 6.3 of the Prohibition of Financing Terrorism Act and Article 57 of the Foreign Trade Act.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

See question 4.1.

4.5 Are there other potential consequences from a criminal law perspective?

From a criminal law perspective, potential consequences include the confiscation of any acquired foreign exchange, securities, asset, real estate, and the like (Article 30 of the Foreign Exchange Transaction Act). Violation of the Act may also lead to a restriction of the foreign exchange transaction (Article 19.2). Restriction on, or revocation of, financial institutions' financing licenses is also a potential consequence (Article 12 of the Financial Investment Services and Capital Markets Act and Article 16 of the Enforcement Decree of the Act, and Article 17 of the Regulations on the Investigation and Sanctions against Financial Institutions).

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

In the case of financial transactions with the Restricted Person due to negligence of employees of a financial institution, the Prohibition of Financing Terrorism Act may impose a fine up to KRW 20 million.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

The FSC is responsible for the investigation and enforcement of civil economic sanctions violations regarding financial transactions with the Restricted Person.

4.8 Is there both corporate and personal civil liability?

There is only criminal liability and no civil liability for violating sanctions under the Foreign Exchange Transaction Act. Under the Prohibition of Financing Terrorism Act, only the financial institution which dealt with the Restricted Person may be liable for civil liability. Under the Foreign Trade Act, both the corporate and natural person can be liable for civil liability.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

Please refer to question 4.6.

4.10 Are there other potential consequences from a civil law perspective?

In case of civil punishment on a financial institution, similar outcomes as explained in question 4.5 may follow.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

During an investigation by the relevant authority, persons or entities subject to such investigations have opportunities to defend themselves by submitting objections. Eventually, the investigating authority determines the level of penalty to be imposed by taking into account the gravity of violation under the relevant laws. Under the Official Information Disclosure Act, all information that is held and managed by public agencies shall be disclosed to the public in principle. However, the Act recognises a wide range of exceptions which includes information pertaining to matters such as management and trade secrets of corporations, organisations or individuals, which if disclosed, may seriously undermine the legitimate interests of them. Therefore, whether such civil enforcement would be disclose to public will depend on specific circumstances of each case.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

The Regulations of Violations of Public Order, which applies to civil penalties, allows a person subject to regulation to challenge the penalty assessments. The court exercises its decision in accordance with Articles 21 and 25 of the Regulation.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

The enforcement is only at the national level.

4.14 What is the statute of limitations for economic sanctions violations?

The statute of limitation for criminal punishment are as follows (Article 249 of the Criminal Procedure Act):

- (i) Ten years for crimes punishable with imprisonment for a maximum term of not less than 10 years.
- (ii) Seven years for crimes punishable with imprisonment for a maximum term of less than 10 years.
- (iii) Five years for crimes punishable with imprisonment for a maximum term of less than five years or a fine.

The statute of limitations for civil penalties is a maximum of five years (Article 19, Act of the Regulation of Violations of Public Order).

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

No additional measures are proposed or under consideration.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

The latest English translations of the Acts and Decrees can be found at the Ministry of Government Legislation's National Law Information Center (<http://www.law.go.kr/LSW/eng/engMain.do>). However, these are not English translations of the current Acts and Decrees, and the current Acts and Decrees are only available at the above website in Korean. The current Acts and Decrees can be searched by using the Korean language as below:

- Foreign Exchange Transaction Act: “외국환거래법”.
- Prohibition of Financing Terrorism Act: “공중 등 협박목적 및 대량살상무기확산을 위한 자금조달행위의 금지에 관한 법률”.
- Foreign Trade Act: “대외무역법”.
- Inter-Korean Exchange and Cooperation Act: “남북교류협력에 관한 법률”.
- Financial Investment Services and Capital Markets Act: “자본시장과 금융투자업에 관한 법률”.
- Enforcement Decree of the Financial Investment Services and Capital Markets Act: “자본시장과 금융투자업에 관한 법률 시행령”.
- Regulations on Designation and Cancellation of Restricted Person on Financial Transactions, etc.: “금융거래등제한대상자 지정 및 지정 취소에 관한 규정”.

The Guidelines and Notices are also available at the above website, but only in Korean which are searchable at the “행정규칙(훈령 예규 고시)” menu.

- Guidelines: “국제평화 및 안전유지 등 의무이행을 위한 무역에 관한 특별조치 고시”.
- Notice of Import and Export of Strategic Items: “전략물자 수출입고시”.
- Notice of Special Measures on Trade to Fulfil Obligations for International Peace Security Maintenance etc. under the Foreign Trade Act: “국제평화 및 안전유지 등 의무이행을 위한 무역에 관한 특별조치 고시”.



Tong-chan Shin is a partner who heads the economic sanctions team and the Middle East desk of the firm. He is also the head of the foreign exchange transaction team of the firm. He served as a member of the policy advisory board for anti-money laundering at the Korea Financial Intelligence Unit under the Financial Services Commission from 2017 to 2019. Currently he is serving as a member of the advisory board of Korea Land & Housing Corporation's Abdulla Smart City Project in Kuwait. He was seconded to Dubai and Abu Dhabi offices of Herbert Smith Freehills from 2012 to 2014 and Dubai office of Trowers & Hamblins from 2014 to 2015. He is a member of the Korean and New York Bars. He obtained his LL.M. degree (*with honors*) from Northwestern University School of Law and LL.B degree (ranked 10th) from Seoul National University College of Law.

Yulchon LLC
Parnas Tower, 38F
521 Teheran-ro, Ganam-gu
Seoul, 06164
Korea

Tel: +82 2 528 5356
Email: tcshin@yulchon.com
URL: www.yulchon.com



Jae Hyong Woo is a partner who specialises in international arbitration and cross-border litigation. Mr. Woo also advises clients on various issues relating to international trade and economic sanctions. Prior to joining Yulchon LLC, Mr. Woo worked at the Korean Ministry of Justice where he focused on trade agreement, investment treaty, and legal service market. Mr. Woo received an LL.M. from London School of Economics and Political Science and was seconded to Pinsent Masons London Office, where he focused on both contentious and non-contentious matters of international construction projects.

Yulchon LLC
Parnas Tower, 38F
521 Teheran-ro, Ganam-gu
Seoul, 06164
Korea

Tel: +82 2 528 5904
Email: jhwoo@yulchon.com
URL: www.yulchon.com



Yong Ju (Ron) Lee is an associate in Yulchon's Corporate & Finance Group and has assisted a number of multinational clients on cross-border transactions. Mr. Lee received a J.D. from Duke University School of Law in 2019 and a B.A. from New York University in 2014.

Yulchon LLC
Parnas Tower, 38F
521 Teheran-ro, Ganam-gu
Seoul, 06164
Korea

Tel: +82 2 528 5607
Email: yongjulee@yulchon.com
URL: www.yulchon.com

Yulchon LLC is a full-service international law firm headquartered in Seoul, Korea with a broad client base comprising major domestic and foreign companies. It employs over 570 professionals, including more than 60 licensed in jurisdictions outside Korea, and has offices in Shanghai, Hanoi, Ho Chi Minh City, Moscow, Jakarta and Yangon. An acknowledged market leader in the development and practice of law, it has three times been named as "The Most Innovative Law Firm in Korea" by the *Financial Times*. It is frequently retained to negotiate complex transactions, help draft new legislation and regulations, and represent clients in high-stakes adversarial proceedings. As one of Korea's premier law firms, Yulchon maintains its high standards of excellence by valuing a culture of collaborative problem-solving.

www.yulchon.com



Attorneys at Law
YULCHON

Netherlands

De Brauw Blackstone Westbroek N.V.



Marlies Heemskerk-de Waard



Marnix Somsen

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

EU Sanctions Regulations have direct effect in the Netherlands, meaning that they are binding on Dutch nationals and legal entities incorporated under Dutch law as well as on Dutch territory. Penalisation of violations and enforcement are provided for in a framework act, the Sanctions Act 1977 (*Sanctiewet 1977*), and a corresponding Sanctions Regulation (*Sanctieregeling*) for each sanctions regime. Pursuant to relevant UN Resolutions and EU law and based on the Sanctions Act 1977, the Netherlands operates a national list of designated parties, whose assets are subject to an asset freeze, the National Terrorism Sanctions List (*Nationale sanctielijst terrorisme*). The Netherlands does not operate any further sanctions regimes in addition to UN and EU sanctions.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

Sanctions are administered by the Ministry of Foreign Affairs. Licences are issued and administered by the Central Import and Export Service (*Centrale Dienst In- en Uitvoer, CDIU*) on behalf of, and in consultation with, the Ministry of Foreign Affairs. Supervision of compliance with sanctions is in the hands of Team POSS (Precursors, Strategic Goods and Sanctions Law), which is part of Dutch Customs. Criminal enforcement is entrusted to the Public Prosecution Service (*Openbaar Ministerie, OM*). Certain sanctions compliance obligations imposed on financial institutions, provided in the Regulation on Supervision pursuant to the Sanctions Act 1977 (*Regeling toezicht Sanctiewet 1977*), are enforced by the Dutch Central Bank (*De Nederlandsche Bank, DNB*) and the Dutch Financial Markets Authority (*Autoriteit Financiële Markten, AFM*).

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

There have been no such changes or developments in the past 12 months.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The Sanctions Act 1977 provides the legal basis for the implementation and enforcement of UN and EU sanctions, as well as the imposition of national sanctions.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes, UN sanctions are implemented by the EU. EU Sanctions Regulations have direct effect in the Netherlands (see question 1.1).

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

- (a) Yes. EU sanctions have direct effect in the Netherlands (see question 1.1).
- (b) No, there are none.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Yes. Parties are added to, and removed from, the National Terrorism Sanctions List by a decision of the Minister of Foreign Affairs, based on the Sanctions Act 1977.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Individuals and entities can lodge an administrative appeal against the decision of the Minister of Foreign Affairs adding them to the National Terrorism Sanctions List.

2.6 How does the public access those lists?

The National Terrorism Sanctions List is available at: <https://www.rijksoverheid.nl/documenten/rapporten/2015/08/27/nationale-terrorisraelijst>.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

No, it does not.

2.8 Does your jurisdiction maintain any other sanctions?

The Netherlands does not maintain any sanctions regimes other than those maintained by the EU.

2.9 What is the process for lifting sanctions?

As the Netherlands does not maintain any sanctions regimes other than those maintained by the EU, this is a matter of EU law. If the EU lifts specific sanctions restrictions, this will have direct effect in the Netherlands, requiring no further action on the national level. If the EU lifts an entire sanctions regime, this will have direct effect as well. In addition, the corresponding national Sanctions Regulation (see question 1.1) will be repealed by the Minister of Foreign Affairs.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes. Export control of dual-use items is primarily regulated at the EU level, pursuant to EU Regulation 428/2009, which is to be replaced by the recast EU Dual-use Regulation 2021/821 on 9 September 2021. Export control of military items is primarily regulated at the national level, while taking into account the EU Common Position 2008/944 and the EU Common Military List. National provisions as to both dual-use and military items are provided in the Strategic Services Act (*Wet Strategische diensten*) and Strategic Items Decree (*Besluit strategische goederen*) and related implementation regulations.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Yes. The EU Blocking Regulation 2271/96, prohibiting adherence to the extra-territorial sanctions regimes imposed by third countries, designated in the Annex to the Regulation, currently including, *inter alia*, US sanctions against Iran and Cuba, has direct effect in the Netherlands (see question 1.1).

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

No, it does not.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

EU sanctions, as applicable in and enforced by the Netherlands, are binding on Dutch nationals and legal entities incorporated under Dutch law, whether acting within or outside the Netherlands, as well as on individuals and legal entities acting in the Netherlands.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Parties are required to freeze funds and assets of individuals or legal entities designated under any EU sanctions or included in the National Terrorism Sanctions List. No economic resources may be made available to such parties.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

EU Sanctions Regulations, as applicable in and enforced by the Netherlands, provide for limited exemptions, authorising certain transactions with sanctioned parties, generally subject to prior authorisation. Such authorisation must be applied for with the Central Import and Export Service.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Various financial institutions, including banks, investment funds, pension funds and insurers, must notify either the Dutch Central Bank or Dutch Financial Markets Authority when, in brief, the identity of one of their relations corresponds to the identity of a person or legal entity designated as a sanctioned party under any applicable sanctions regulations. The notification must include the identity of the relation. The term "relation" includes everyone involved in a financial service or transaction and thus extends beyond the direct contractual counterparty of the financial institution.

For both financials and non-financials, licences for transactions that would otherwise be restricted pursuant to economic sanctions may provide for reporting obligations. Otherwise, no reporting obligations apply.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

The Ministry of Foreign Affairs has published "Guidelines for compiling an Internal Compliance Programme for Strategic Goods, Torture Goods, Technology and Sanctions" (the "ICP Guidelines"), which are available in both Dutch and English at <https://www.rijksoverheid.nl/documenten/richtlijnen/2019/02/22/richtlijnen-opstellen-internal-compliance-programme>. The ICP Guidelines are structured around seven

core elements: (i) commitment to compliance; (ii) structure and responsibility; (iii) export screening procedure; (iv) shipment control; (v) training; (vi) audit, reporting and improvement measures; and (vii) archiving. An internal compliance programme (ICP) is required to obtain a global licence, which is valid for multiple transactions concerning one or more types of items to one or more destinations.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes. National Sanctions Regulations, enacted pursuant to the Sanctions Act 1977, prohibit violation of EU Sanctions Regulations. Violation of such National Sanctions Regulations constitutes a violation of the Sanctions Act 1977, which in turn constitutes an economic offence and is punishable under the Economic Offences Act (*Wet op de economische delicten*).

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

Criminal enforcement of sanctions is the responsibility of the Public Prosecution Service. The Public Prosecutor may involve both Team POSS (see question 1.2) and the Fiscal Intelligence and Investigation Service (*Fiscale inlichtingen- en opsporingsdienst, FIOD*) to investigate a matter. The decision to prosecute or not remains with the Public Prosecutor.

4.3 Is there both corporate and personal criminal liability?

Yes. Both individuals and legal entities can be held criminally liable for violations of sanctions.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

If the violation was committed wilfully, it is considered a serious offence (*misdrif*), in which case the following financial penalties can be imposed:

- On individuals:
 - a fine of the 5th category; or
 - if the value of the relevant goods exceeds one fourth of the maximum fine in the 5th category, a fine of the 6th category.
- On legal entities:
 - a fine of the 6th category; or
 - if a fine can be imposed of the 6th category, but the maximum fine in that category is considered insufficient, a fine of up to 10% of the annual turnover of the legal entity in the year before the imposition of the penalty order (only in relation to offences committed on or after 1 January 2015).

A fine of the 5th category currently amounts to EUR 87,000. A fine of the 6th category currently amounts to EUR 870,000. These amounts are adjusted for inflation every two years.

4.5 Are there other potential consequences from a criminal law perspective?

Other potential consequences include:

- imprisonment;
- community service;
- disgorgements;
- debarment; and
- licence revocation.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

This is not applicable as the Netherlands does not have a civil enforcement practice comparable to that of, for example, the U.S.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

This is not applicable.

4.8 Is there both corporate and personal civil liability?

This is not applicable.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

This is not applicable.

4.10 Are there other potential consequences from a civil law perspective?

This is not applicable.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

This is not applicable.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

This is not applicable.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal enforcement of sanctions occurs at national level only.

4.14 What is the statute of limitations for economic sanctions violations?

Minor offences (*overtredingen*) become time-barred three years after the relevant offence was committed. Serious offences

(*misdrijven*), i.e. wilfully committed offences (including conditional intent), only become time-barred 12 years after the relevant offence was committed.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

The Dutch Central Bank has pleaded, and the Minister of Finance has promised to investigate the possibilities for the introduction of a legal ground for the obligatory publication of administrative enforcement measures, such as financial penalty decisions, against financial institutions on the basis of the Sanctions Act 1977. Such legal ground is currently lacking, as a result of which economic enforcement measures taken by the Dutch Central Bank or the Dutch Financial Markets Authority against financial institutions are not published.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Relevant laws and regulations can be found at <https://wetten.overheid.nl>, but are not available in English.

Some high-level general information on sanctions, provided by the Dutch government and available in English, can be found at: <https://www.government.nl/topics/international-peace-and-security/compliance-with-international-sanctions>.

Some further information is also provided by the Central Import and Export Service and available in English at: https://www.belastingdienst.nl/wps/wcm/connect/bldcontenten/belastingdienst/customs/safety_health_economy_and_environment/cdiu_cluster/sanctions/.



Marlies Heemskerk-de Waard advises clients on all aspects of economic sanctions as well as export controls and other international trade matters, ranging from training and compliance advice to the assessment and structuring of actual trade transactions, involving sanctioned countries or strategic items. Marlies has conducted multiple internal investigations into international trade-related matters and represented corporates *vis-à-vis* both national and international enforcement authorities in relation to such matters. She also regularly advises on international trade-related issues in the context of M&A transactions. Her experience includes two years with the firm's New York office, assisting clients subject to US enforcement in a variety of matters, including economic sanctions and export controls.

De Brauw Blackstone Westbroek N.V.
 Claude Debussylaan 80, 1082 MD
 Amsterdam
 The Netherlands

Tel: +31 20 577 1702
 Email: marlies.heemskerk-dewaard@debrauw.com
 URL: www.debrauw.com



Marnix Somsen specialises in regulatory and criminal enforcement. He represents corporations and financial institutions subject to investigation and enforcement proceedings. Marnix assists our clients in cases regarding national and international trade, economic sanctions and export control regulations. Marnix typically handles cross-border enforcement matters and internal investigations for EU companies involving one or more US or other foreign regulators, drawing upon the resources of our international Best Friends network.

De Brauw Blackstone Westbroek N.V.
 Claude Debussylaan 80, 1082 MD
 Amsterdam
 The Netherlands

Tel: +31 20 577 1628
 Email: marnix.somsen@debrauw.com
 URL: www.debrauw.com

De Brauw assists clients with a broad range of cutting-edge complex international trade, economic sanctions and export control matters. In doing so, we provide effective solutions which align business goals with legal requirements.

We advise on the permissibility of transactions and the applicability of license requirements and other restrictions. We regularly conduct internal investigations and have ample experience in assisting clients in economic sanctions and export control related (cross border) enforcement matters.

We offer in depth knowledge of the regulatory and criminal enforcement landscape demonstrated by our extensive experience in assisting clients *vis-à-vis* various authorities, including the Dutch Ministry of Foreign Affairs, Team POSS, the Central Import and Export Service (CDIU) and the Dutch Public Prosecutor (OM), as well as the US Office of Foreign Assets Control (OFAC), the Bureau of Industry and Security (BIS) and the Department of Justice (DoJ).

Together with our M&A and Competition colleagues, we furthermore advise on transactions and foreign direct investment screening relating to strategic investments, notably those involving sensitive technologies.

www.debrauw.com

DE BRAUW
 BLACKSTONE
 WESTBROEK

Norway

Kluge Advokatfirma AS



Ronny Rosenbold



Siri Fosse Sandve

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Norway maintains a variety of sanctions, ranging from comprehensive to more limited restrictions. Norway generally implements sanctions pursuant to UN and EU sanctions, and also OSCE arms embargoes (for example, on Azerbaijan). UN and EU sanctions measures must be implemented in Norwegian legislation before they can be made binding on private legal entities in Norway.

However, the Norwegian Parliament may implement sanctions autonomously and may also implement UN and EU sanctions with national amendments. By way of example, Saudi Arabia is currently under restrictions, which means that no exports of military or dual-use items are permitted for military use.

Norway also generally extends the application of sanctions to overseas territories such as Svalbard and Dronning Maud Land. Norwegian sanctions do not purport to have an extra-territorial effect on actions outside Norway, although they do apply to Norwegian nationals, companies established under Norwegian law and Norwegian aircraft/vessels, wherever located.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The Norwegian Ministry of Foreign Affairs (MFA) administers and enforces the sanctions regime. The MFA has broad oversight for sanctions policy in Norway. A subgroup under the MFA, the Section for Export Control, administers the applications based on Norwegian legislation.

According to the Police Act, the Norwegian Police Security Service (PST) shall prevent, investigate and prosecute violations of the sanction regimes. The Financial Supervisory Authority (FSA) has a mediating role in the work on sanctions and freezing obligations. This entails the dissemination of listing records from the UN and the EU to enterprises that are subject to supervision by the FSA. The Norwegian Customs has tasks regarding the control of goods, enforcement, prevention and investigation of the violation of export regulations.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

Norway has adopted a new Act on the Implementation of International Sanctions (the Sanctions Act). The Sanction Act

applies both to the implementation of binding sanctions under international law adopted by the UN Security Council and to the implementation of other non-military measures with broad international support, which Norway supports. The latter has in practice so far been limited to restrictive measures adopted by the EU. Even though a new Sanctions Act has been adopted, most relevant legislation is to be found in several regulations that has not been changed.

Pursuant to the new Sanctions Act Norway has implemented the following three regulations adopted by the EU in 2021:

- Council Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks;
- Council Regulation (EU) 2018/1542 concerning restrictive measures against the proliferation and use of chemical weapons; and
- Council Regulation (EU) 2020/1998 concerning restrictive measures against serious human rights violations and abuses.

Another interesting development is a royal decree issued on 26 March 2021: the government ordered that Rolls Royce stop the sale of Norwegian company Bergen Engines AS to companies within the Transmashholding Group. Based on publicly available information and media coverage, the government concerns relate to the Russian ownership. This is the first time that an acquisition has been stopped on this basis and is therefore interesting from a sanction's perspective. In Norway, the jurisdiction to review foreign investments on national security grounds is vested in the Security Act. Undertakings that handle classified information, control or engage in activities of vital importance to national functions can be made subject to reporting requirements under the Act and, if so, must be explicitly notified by decision (*cf.* Section 1-3). Where a third party wishes to acquire a "qualified interest" in an undertaking subject to the Act, a notification must be submitted to the National Security Authority (*cf.* Section 10-1). In turn, if the acquisition presents a "not insignificant" risk of a threat to national security interest, the government can either block the transaction or authorise it subject to commitments (*cf.* Section 10-3). But also, companies where there is no formal decision may be stopped from being acquired if the interest of national security is threatened (*cf.* Section 2-5).

Finally, we may add that the transition period for Brexit is over. The United Kingdom and Northern Ireland are no longer parties to the EEA agreement, and are therefore treated as other third countries. Most relevant in this regard is probably that the Norwegian Export Control Regulations on "Exports of defense-related goods to recipients in the EEA" no longer applies to the UK.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The Norwegian sanctions regime is based on national legislation administered by the MFA, Section for Export Control. Sanctions that are adopted by the UN Security Council (UNSC) and EU restrictive measures and other international non-military measures with which Norway has aligned itself are implemented through regulations under the new Act of 16 April 2021 No. 18 on the Implementation of International Sanctions (the Sanctions Act). This differs from the past where UNSC and EU sanctions were implemented under different national acts.

More detailed provisions laid down by the MFA are found in regulations adopted under the Sanction Act that provide the legal authority for such measures.

In April 2018, the MFA published updated guidelines on financial sanctions. The purpose of the guidelines is to provide information that will make it easier to understand the financial restrictions in the Norwegian regulations, which are based on UNSC sanctions and EU restrictive measures. The guidelines only provide general information and are not legally binding for the MFA in their interpretation of the current regulation.

Certain types of measures included in UN sanctions and/or EU restrictive measures are implemented under other Norwegian legislation. These include travel restrictions, which are implemented under the immigration legislation, and arms embargoes, which are often implemented under the ordinary export control legislation. Thus, only some of the Norwegian regulations on sanctions and restrictive measures expressly mention arms embargoes.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

If the UNSC determines that an act of aggression or a breach of peace has occurred, it may decide what measures member states must take in order to restore or maintain international peace and security. Norway is obligated under international law to implement UNSC's binding resolutions. UN resolutions do not, however, have a direct effect in Norway and they must be implemented in Norwegian legislation before they can be made binding on persons and entities in Norway. Norway's Sanctions Act enables the Government to give effect to decisions passed by the UNSC. Before a resolution is implemented into national law, a Norwegian regulation must be drafted.

As of today, Norway has implemented the current UNSC resolutions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

Norway is part of the Agreement on the European Economic Area (the EEA Agreement), which brings together the EU Member States and the three EEA EFTA States (Norway, Iceland, and Lichtenstein). Foreign policy falls outside the scope of the EEA Agreement, and Norway is therefore not bound by or obligated to implement EU sanctions. When the

EU adopts new restrictive measures, the MFA makes an assessment and the Norwegian Government decides whether Norway shall follow the EU measures. The Government tends to follow the EU in this regard.

We emphasise that when implementing EU regulations, national adjustments are included, so the implemented regulations are in fact not a blueprint of the EU regulations and establish Norwegian autonomous regimes. This has the consequence that one may not base a legal assessment on EU legislations.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Norway largely adopts the list contained in the corresponding UNSC resolutions and/or EU regulations, which are implemented as described under questions 2.2 and 2.3.

The list of sanctioned individuals and entities is found in Norwegian regulations. The regulations either include a list of designated parties or refer to a list updated by the UN or the EU. As an example, we may refer to the Norwegian Regulation of 15 August 2014 No. 1076 on restrictive measures against Russia, which implements the EU's restrictive measures. Previously, the national regulation included a list of individuals and entities that was updated by the MFA. With effect from 2017, the MFA revised the regulation, and it now only refers to the applicable EU consolidated list of sanctioned persons and entities. An exemption is the Norwegian Regulation of 15 December 2015 No. 2103 on restrictive measures against Venezuela where Norway has adopted a national entity list.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

If a person or entity considers a listing to be unlawful, it is possible to request a "delisting" (to be removed from the list). The delisting processes are different for UN and EU listings and are described below.

In recent years, the UNSC has adopted procedures and guidelines for listing and delisting. A petitioner seeking to submit a request for delisting from the UN sanctions list can do so directly, or through a representative, by contacting the UN Office of the Ombudsperson. In Norway, the MFA may assist any listed persons with requests for the removal from the lists. Such assistance may also be provided by lawyers with relevant expertise.

The EU Council shall warn persons and entities subject to freezing restrictions or travel restrictions under restrictive measures. At the same time, the Council shall inform such persons about the possibility of legally testing the validity of a listing. When a person or entity wants to challenge a listing measure, such as its inclusion on a sanctions list, it has two principal procedures at its disposal. These procedures are either an administrative-review procedure by the Council or challenging the listing in the European Court of Justice. Several individuals and entities have, in recent years, successfully challenged the listing. Most of these court cases involved a lack of respect for procedural fundamental rights (rights of defence, due process), mostly relating to administrative and procedural deficiencies. For example, a June 2014 court decision annulled the listing of Syria International Islamic Bank for insufficient grounds, where the listing was based mainly on allegations that the bank had permitted other listed banks to circumvent EU sanctions by

facilitating transactions for their (non-listed) account holders (*cf.* Case T-293/12).

It can be questioned whether the listing of an individual or entity can be challenged in front of the national courts. Norway is obligated through its UN membership to implement the UNSC's listings. We cannot therefore see how such listings may be challenged in front of the national courts. However, the same obligation to implement the listing from the EU does not apply. Implementations of the EU's listings of individuals or entities are based on a national decision, normally conducted by the MFA. Such a decision shall follow the ordinary rules under the Public Administration Act of 10 February 1967. If procedural rules are not followed, the decision may be challenged in front of the court.

Objections may also be raised against the banks that are freezing assets. Objections may be brought in front of the court, e.g. on the basis that a bank has frozen assets that are not covered by the regulation.

2.6 How does the public access those lists?

There are no consolidated versions of listed persons and entities. The MFA do, however, keep an updated list with references to current legislation on their webpage: <https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/sanksjoner-og-tiltak/sanksjoner-og-tiltak/id2008477/> (in Norwegian only).

The EU Sanctions Map, including both EU restrictive measures and UN sanctions, is a useful source of information, since Norway essentially has similar sanction rules: <https://www.sanctionsmap.eu/>. We do, however, emphasise that it is the Norwegian regulations that apply in case of differences.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Norway maintains comprehensive sanctions against countries and regions, such as Crimea/Sevastopol and North Korea.

In addition to the comprehensive sanctions, Norway also maintains an arms embargo for 17 countries.

2.8 Does your jurisdiction maintain any other sanctions?

Norway is currently maintaining sanctions against 26 different nations, geographical areas and terrorist organisations. In response to the consequences of comprehensive sanctions on civilians, “targeted” or “smart” sanctions are more often used. These targeted sanctions are conceived to directly affect the political leaders or those responsible for human rights violations. Properly targeting sanctions, it is hoped, can eliminate civilian suffering while putting significant pressure on the Government itself, thus bringing sanctioned regimes into compliance with human rights and humanitarian law and increasing their chances of success.

Targeted financial sanctions are most commonly used in Norwegian legislation. This includes freezing the assets of persons or entities listed under national sanctions regulations. Listed persons may also be subject to travel restrictions. Norway also applies trade restrictions on goods, normally those such as arms, dual-use goods and goods which could be used in enrichment-related activities, such as oil, natural gas, petrochemical and petroleum products.

2.9 What is the process for lifting sanctions?

In Norway, the lifting of national sanctions can be quite straightforward. If the sanctions were imposed by a national regulation under the Government's authority, they can be lifted quite quickly under that same authority. If sanctions are imposed, in whole or in part, on the basis of an act passed by Parliament, the sanctions must be lifted by Parliament and that will normally take longer. It also requires that the majority of parliament accepts to lift the sanctions.

The sanctions which are imposed by the UNSC are binding for Norway under international law. Lifting such sanctions can only be carried out when the UNSC resolution is lifted, otherwise it will be a breach of Norway's obligations as a member of the UN.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Norway has an export control regime applicable to the export of military and dual-use equipment. The export control regime is applicable even when it is exported to “friendly” countries like those in the EU or NATO allies. Such items cannot be exported without a licence from the MFA.

The MFA is the authority responsible for the control of exports of weapons, ammunition and other military equipment, dual-use items and relevant technology and services from Norway. The law governing export control is the Act of 18 December 1987 relating to Control of the Export of Strategic Goods, Services, Technology, etc. (the Export Control Act). The Export Control Act provides the authority to regulate exports of all goods, services and technology that may be of significance for another country's development, production or utilisation of products for military use. It also regulates goods, services and technology that may directly serve to develop a country's military capability, including goods and technology that can be used to carry out terrorist acts.

More detailed provisions laid down by the MFA are found in the regulation dated 19 June 2013 relating to the export of defence-related products, dual-use items, technology and services (the Export Control Regulation). The Export Control Regulation provides the operational legal framework for the MFA's implementation of export controls, including licensing requirements.

The control lists form part of the Export Control Regulation and specify the goods and technology for which an export licence is required. The two lists are for defence-related products (List I) and dual-use items (List II). Control of technology also includes control of intangible transfers of technology. In practice, the lists are the result of negotiations in the multilateral export control regimes of which Norway is a member. The lists are regularly maintained. Products that are listed require a licence prior to export.

The Export Control Regulations also contain several so-called general clauses (“catch-all”). These controls provide a regulatory basis to require the MFA's permission to export unlisted items when there is a reason to believe such items are intended for such as biological and nuclear weapons, but it may also cover other purposes of end-use.

The obligation to provide an export licence is linked to the time of “export”, *cf.* the export control regulation of 2013, section 2 No. 3. In Norway, some of the technology used for oil and gas production and exploration is controlled. However, the Export Regulation considers the continental shelf as a part

of Norway and there is no need to apply for a licence when sending technology or equipment from the mainland to installations offshore. A licence is needed when it leaves the Norwegian economic zone. The geographical scope of the export control regulations was expanded in 2021 and now also applies to Svalbard and Jan Mayen.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Norway does not have blocking statutes, for example such as you find in the EU, which are intended to hinder the application of a law made by a foreign jurisdiction.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

Norway does not impose secondary or extraterritorial sanctions which target non-Norwegian entities or persons that transact with sanctions targets outside the Norwegian jurisdiction.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

Generally, the Norwegian sanctions regulations apply:

- a) within the territory of Norway, including Norwegian airspace;
- b) on board any aircraft or vessel under Norwegian jurisdiction;
- c) *vis-à-vis* all Norwegian nationals irrespective of their location;
- d) *vis-à-vis* all legal persons, entities and bodies established in accordance with Norwegian law; and
- e) *vis-à-vis* all legal persons, entities and bodies with regard to the business activities they conduct wholly or partly in Norway.

The type of transactions covered by the sanctions regulations are specified in each regulation, which generally corresponds with the UN sanctions and EU restrictive measures.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Under the Norwegian economic sanction regime, individuals and legal entities are obliged to block and/or freeze funds or other assets which directly or indirectly belong to or are under the control of persons, units or groups listed in the specific sanctions regulations. Generally, these Norwegian regulations correspond with the UN sanction lists and EU restrictive measures. The Norwegian Penal Code also regulates the seizure of assets belonging to individuals or legal entities involved in terrorist acts.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Generally, the Norwegian regulations provide the MFA with a right to grant exemptions from the sanction's regulations in accordance with the relevant UN sanctions or EU restrictive measures. The MFA may also grant exemptions in special cases where the regulation has a clear unintended effect, provided that the exemption does not conflict with Norway's international law obligations or the motives behind the measures.

Under the Export Control Regulation, the following are prohibited without a specific licence:

- i) exporting of certain listed goods and technology;
- ii) provision of services related to the listed goods and technology;
- iii) other services which can serve to develop another country's military ability and trading brokering; and
- iv) assisting in the sale of certain goods, technology or services.

Licences are issued by the MFA.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

In Norway, there are no general sanctions-related reporting requirements.

Under the Norwegian export control and licensing regime, exporters and other persons assisting in the trade of certain goods and services must, however, report certain information regarding its transactions to the MFA in order to obtain an export licence (for instance: the type of goods; the quantity and value; transfer date; the name and address of the supplier and the consignee; and the end-user and end-use of the goods, etc.).

Furthermore, suppliers are also obliged to report on all exports and transfers of listed military/defence-related goods. The reports shall be sent to the MFA on a prescribed form each quarter.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

Generally, legal entities are not required by law to maintain a compliance programme. The exceptions are banks, insurance companies, investment funds, accountants and other financial institutions which are required to have a compliance programme that shall include internal regulations on screening customers and customer databases against persons, units or groups listed in the sanctions regulations (know-your-customer requirements).

Entities who are exposed to different sanctions regimes on a more regular basis are, however, expected to have internal guidelines, instructions, training, checks or other measures in place to ensure compliance with the sanction regulations. This follows on from the fact that the use of such measures is considered when assessing the size of a financial penalty (see question 4.4 below). The Norwegian authorities have also issued non-binding guidelines regarding the obligation to block and freeze funds or other property that violate sanctions prohibitions.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

A violation of economic sanction laws and regulations is punishable by imprisonment (of up to three or five years), financial penalties and/or confiscation. A legal entity found guilty of violating economic sanctions can also lose the right to operate its business, or may be prohibited from operating in certain forms. Depending on the act, a violation of economic sanction laws and regulations could also be covered by sections of the Norwegian Penal Code with higher maximum penalties (such as chapter 18 on terrorist acts and terrorism-related acts).

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The PST is responsible for investigating and prosecuting criminal economic sanctions offences. Criminal sanction cases are often referred to the PST by the MFA.

4.3 Is there both corporate and personal criminal liability?

In accordance with Norwegian criminal law, both legal entities and individuals may be found liable for breach of economic sanctions regulations.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

There are no fixed maximum levels of financial penalties for individuals or legal entities convicted of criminal violation of sanctions. The financial penalties are set by a court of law based on an overall assessment.

For legal entities, the following circumstances shall be taken into consideration as part of the overall assessment:

- a) the preventive effect;
- b) the severity of the offence, and whether a person acting on behalf of the legal entity has acted culpably;
- c) whether the entity could have prevented the offence by use of guidelines, instruction, training, checks or other measures;
- d) whether the offence has been committed in order to promote the interests of the legal entity;
- e) whether the legal entity has had or could have obtained any advantage by the offence;
- f) the financial capacity of the legal entity;
- g) whether other sanctions arising from the offence are imposed on the legal entity or a person who has acted on its behalf, including whether a penalty is imposed on any individual person; and
- h) whether agreements with foreign states prescribe the use of enterprise penalties.

For individuals, the main factors in assessing the size of financial penalties are: the preventative effect; the severity of the offence; proportionality; and the offender's financial situation (income, assets, responsibility for dependents, debt burden, and other circumstances affecting financial capacity).

4.5 Are there other potential consequences from a criminal law perspective?

Yes. An example is withdrawal of proceeds from criminal action.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

In Norway, violations of economic sanction laws and regulations are penalised through criminal penalties and the criminal justice system (*cf.* questions 4.1–4.4 above). There is no civil enforcement institute in Norway. There are, however, certain consequences that are not considered criminal penalties under Norwegian law:

- The MFA may revoke, suspend or restrict an already issued export licence if the licence is abused, the terms of the licence are breached and/or in case of violation of the export control regulations. A breach of the economic sanctions regulations can also affect a company's ability to obtain another export licence.
- The MFA may issue a daily fine if a legal entity or person does not comply with the duty to provide information to the MFA.
- A court of law may also seize goods that have been exported, imported or sought to be exported/imported in violation of the UN sanctions regulations. The same applies to means of payment and securities used. If the goods, funds or securities cannot be confiscated, the value may be seized.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

This is not applicable in Norway.

4.8 Is there both corporate and personal civil liability?

This is not applicable in Norway.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

This is not applicable in Norway.

4.10 Are there other potential consequences from a civil law perspective?

This is not applicable in Norway.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

This is not applicable in Norway.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

This is not applicable in Norway.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal enforcement of economic sanctions laws and regulations is handled at a national level by the PST, the MFA and the Norwegian Customs.

4.14 What is the statute of limitations for economic sanctions violations?

The statute of limitations for criminal enforcement of economic sanctions violations depends on the maximum statutory penalty prescribed. The limitations period is five years when the maximum statutory penalty is imprisonment for three years. The limitation period is generally calculated from the day the offence ceased. If a person or legal entity has committed several offences of the Norwegian Penal Code through the same act, the longest limitation period applies to all the offences.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

The Norwegian sanctions regime generally corresponds with the UN sanctions list and EU restrictive measures. There are currently no indications that the Norwegian Government will propose any unilateral sanctions.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

The Norwegian Government has prepared a list of relevant sanction laws and regulations on their website (<https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/sanksjoner-og-tiltak1/sanksjoner-og-tiltak/id2008477/>). The sanction laws and regulations are available in Norwegian on the Norwegian public database for legal resources – <https://www.lovdatab.no>.

The Norwegian sanctions regime is, however, largely based on EU restrictive measures and the UN sanctions regime. The EU web portal (<https://www.sanctionsmap.eu/#/main>), which provides a visual overview of EU and UN restrictions, is therefore recommended as a useful source of information. The MFA also issues an annual white paper to the Norwegian Parliament on Norwegian Exports of Defence-related Products, Export Control and International Non-proliferation Cooperation. A summary of this paper is available in English at https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/eksportkontroll/meldst25_-2019_2020_engsummary.pdf.

Useful information regarding the Norwegian export control regime is also available at the following government website: <https://www.regjeringen.no/en/topics/foreign-affairs/eksportkontroll/id754301/>.



Ronny Rosenvold is an experienced lawyer dedicated to providing legal assistance within the field of export control and sanctions regulations. Mr. Rosenvold is one of few Norwegian lawyers who have significant experience within international trade, sanctions and export control. He has considerable experience representing individuals facing restrictive measures, as well as corporations requiring compliance and litigious advice arising from the enforcement of sanctions.

Rosenvold also has broad experience as a legal advisor for Norwegian and international companies in complex cases within different areas of EU/EEA law.

His practice includes different sectors, but particularly in the fields of technology, industry, energy and defence.

Kluge Advokatfirma AS

Bryggegate 6
0250 Oslo
Norway

Tel: +47 908 96 993

Email: ronny.rosenvold@kluge.no

URL: www.kluge.no



Siri Fosse Sandve is an experienced lawyer who specialises in Norwegian petroleum and energy law. She assists Norwegian and international clients with legal advice on the Norwegian oil and gas sector, as well as international trade, sanctions and export control issues particularly related to the energy sector. Ms. Sandve has assisted businesses in communication with Norwegian authorities regarding the export of listed items. She has also assisted Norwegian companies in developing internal compliance regulations.

Kluge Advokatfirma AS

Olav Kyrres gate 21 (Herbarium)
NO-4005 Stavanger
Norway

Tel: +47 915 81 528

Email: siri.fosse.sandve@kluge.no

URL: www.kluge.no

Kluge is a full-service independent law firm with offices in Oslo, Stavanger, Bergen and Hamar. Kluge offers comprehensive advice and assistance within all major fields of business law.

Kluge is recognised in *The Legal 500* and *Chambers and Partners* in all of Kluge's practice areas.

Kluge's broad range of legal services includes: corporate; dispute resolution; compliance; real estate and construction; labour law; banking and finance; public procurement; IPR; as well as data protection, digitalisation, information technology and telecommunications.

Kluge is the preferred partner for many of the most important players in their selected markets, and they have a solid international network. Kluge has a broad range of long-term clients, ranging from international E&P and oil service companies, key governmental bodies, large construction/infrastructure companies, investment banks, investors, private equity funds, to local businesses in Norway.

www.kluge.no



KLUGE

Russia

Rybalkin, Gortsunyan & Partners



Oleg Isaev



Anastasia Konstantinova



Marina Abazyan

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Russia may impose special economic measures in order to ensure the security and safety of the Russian Federation and/or to protect the interests of Russian citizens.

Currently the following main restrictions have been implemented in Russia: (1) measures imposed by the United Nations Security Council Resolutions (the “UN Sanctions”); (2) an import ban in relation to certain products from Albania, Australia, Canada, the EU, Iceland, Lichtenstein, Montenegro, Norway, Ukraine, the United Kingdom of Great Britain and Northern Ireland, Turkey and USA; (3) a restriction on the export of certain products to Ukraine; (4) the blocking (freezing) of funds (property) of certain individuals and entities related to Ukraine; (5) a travel ban in relation to certain individuals from Canada, the EU and USA; (6) sanctions related to certain U.S. citizens; (7) sanctions related to international or foreign non-governmental organisations; (8) an air travel ban in relation to Georgia and Ukraine; and (9) a restriction on hiring by diplomatic missions, consulates, representative offices or other state authorities of USA and Czech Republic of individuals located in the Russian Federation.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The decision on imposing and abolishing sanctions is made by the President of the Russian Federation upon proposals of the Security Council, the Federation Council and/or the State Duma of the Russian Federal Assembly or the Government.

The Government of the Russian Federation implements the sanctions imposed by the President by determining specific measures and restrictions. Where necessary the Central Bank of Russia is also involved in the implementation of restrictive measures.

Depending on the type of sanctions, other federal authorities are also responsible for administering and enforcing sanctions. For example, the restrictions related to the import of goods are mainly enforced by customs authorities.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

Restrictions on media platforms

On 10 January 2021, certain amendments were introduced to Federal Law No. 272-FZ dated 28 December 2012 “On measures against persons involved in violation of fundamental human rights and rights of citizens of the Russian Federation” (“Law No. 272”), pursuant to which Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (“Roskomnadzor”) shall maintain a list of owners of internet media platforms that are limiting access to information deemed publicly important to the Russian Federation, including, *inter alia*, by way of discrimination on the basis of ethnicity, language, origin, occupation, religion and/or in connection with sanctions imposed by foreign countries against Russia, Russian citizens or entities. Roskomnadzor can restrict access to such media platforms.

Hiring restrictions

On 23 April 2021, Decree of the President of the Russian Federation No. 243 “On measures (counter-measures) in response to inimical actions of foreign countries” (“Decree on counter-sanctions”) has been passed imposing a restriction on hiring by diplomatic missions, consulates, representative offices or other state authorities of foreign countries of individuals located in the Russian Federation. The list of countries falling under such restrictions as well as the number of individuals that can be hired is introduced by Russian Government. Currently the restrictions apply to the United States of America and to the Czech Republic.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Legal grounds for imposing sanctions in Russia are the following: the Constitution of the Russian Federation; the principles and rules of international law; international treaties to which Russia is a party; Federal Laws; Presidential Decrees and Governmental Resolutions; and other acts of federal government authorities.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Russia implements the UN Sanctions. Based on a general provision on the implementation of the principles and rules of international law set forth in the Russian Constitution, and in accordance with the Federal Law No. 281-FZ dated 30 December 2006 “On special economic measures and coercive measures” (the “Sanctions Law”), the United Nations Sanctions are implemented by decrees of the President of the Russian Federation and by the Federal Law No. 115-FZ dated 7 August 2001 “On anti-money laundering and countering terrorism financing” (the “AML and CFT Law”).

There are no significant ways in which Russia fails to implement UN Sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

No regional body of which Russia is a member has issued sanctions. However, in accordance with the Eurasian Economic Union Treaty (to which Russia is a party) the Eurasian Economic Union is, in principle, entitled to introduce measures in relation to third states that may have an impact on international trade activities, such as increase on import customs duty, setting quantity restrictions and similar measures.

In addition to the above, Russia and Belarus are parties to a treaty “On creation of a Union State” dated 8 December 1999, pursuant to which the parties may develop unified legislation on measures for protection of rights of their citizens and entities.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Yes, Russian authorities maintain lists of sanctioned entities and individuals. However, the procedures for maintaining and altering such lists are different depending on the type of sanctions.

Ukrainian Sanctions. Certain restrictions are introduced in relation to individuals and entities related to Ukraine (“Ukrainian Sanctions”) under Decree of the President of the Russian Federation dated 22 October 2018 No. 592 “On implementation of special economic measures in connection with inimical actions of Ukraine in relation to Russian citizens and legal entities” (as amended) (“Presidential Decree No.592”).

A list of sanctioned individuals and legal entities is introduced and maintained by the Russian Government. Currently such list contains 849 individuals and 84 legal entities and is attached to the Governmental Resolution No. 1300 dated 1 November 2018 “On measures for implementation of Decree of the President of the Russian Federation dated 22 October 2018 No. 592” (the “Governmental Resolution No.1300”) (as amended). According to the Governmental Resolution No. 1300 the Russian Ministry of Finance is entitled to propose amendments to the list of sanctioned persons; however, any alteration of such list shall be introduced by a Governmental Resolution.

UN Sanctions. The list of sanctioned persons is introduced by the relevant UN Security Council Resolution and repeated in a Presidential Decree implementing such Resolution in Russia.

The Federal Financial Monitoring Service of Russia (“Rosfinmonitoring”) maintains lists of individuals and entities which appear to be involved in extremism and terrorism or involved in the proliferation of weapons of mass destruction based on the lists introduced by relevant Security Council Resolutions (“Rosfinmonitoring lists”).

The procedure for amending such lists of sanctioned persons is set forth in the relevant UN Security Council Resolutions and relevant Committee Guidelines and is available on the website of the relevant committee. In case a list of sanctioned persons is amended, the Presidential Decree implementing the respective sanctions and the list maintained by Rosfinmonitoring are amended accordingly.

Sanctions against U.S. citizens and travel bans. According to publicly available statements of the Ministry of Foreign Affairs of Russia imposed a travel ban on certain individuals who are U.S., EU, and Canadian officials.

Lists of individuals who are subject to the travel ban are published from time to time by the Ministry of Foreign Affairs. However, neither the full list of individuals, nor the procedure for amending such lists, except for the list of individuals falling under restrictions introduced by Law No. 272, are publicly available.

The list of U.S. citizens that are subject to restrictions under Law No. 272 can be amended pursuant to a proposal by the senators of the Federation Council of the Federal Assembly, members of State Duma of the Federal Assembly, the Ombudsman, Civic Chamber, political parties and governmental bodies.

Sanctions related to international or foreign NGOs. Pursuant to Law No. 272 certain international or foreign non-governmental organisations (“the NGOs”) that threaten the foundations of the constitutional order or security of Russia are considered unwanted. Any transaction with funds and/or other property of NGOs included in the list maintained by the Russian Ministry of Justice shall be blocked by financial institutions. Alternations of the list are made by the Ministry of Justice on the basis of information received from the General Prosecutor.

Media platforms. As described above, upon the decision of the General Prosecutor of Russia agreed with the Ministry of Foreign Affairs of the Russian Federation, Roskomnadzor maintains a list of owners of internet media platforms that limit the access to information deemed publicly important in the Russian Federation (“List of media platforms”). Roskomnadzor notifies the owners of such media platforms that they are in violation of Law No. 272 and, if the owner of the media platform does not comply with the demands of Roskomnadzor, limits the access to such media platform.

In case the foreign media platform is no longer in violation of Law No. 272, Roskomnadzor shall provide the information on such media platform to the General Prosecutor. Once such information is received by the General Prosecutor, he/she (in agreement with the Ministry of Foreign Affairs) shall cancel the measures and inform Roskomnadzor. Restrictions shall be lifted by Roskomnadzor within one day following notification by the General Prosecutor.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

No specific procedure for challenging the listing in a sanctions list is set out in relation to the Ukrainian Sanctions, travel bans, NGOs and other sanctions that may be imposed under the Sanctions Law and/or Counter-Sanctions Law.

In the case that a person is mistakenly included in the lists maintained by Rosfinmonitoring, such person may file an application for delisting with Rosfinmonitoring.

2.6 How does the public access those lists?

The list of sanctioned persons in relation to the Ukrainian Sanctions is attached to the Governmental Resolution No. 1300 and available on the Russian website containing official texts of legal acts (<http://pravo.gov.ru>).

The lists of sanctioned persons in relation to the UN Sanctions are available on the official website of UN Security Council (<https://www.un.org/securitycouncil/sanctions/information>).

The lists maintained by Rosfinmonitoring are published in the newspaper “Rossiyskaya Gazeta” and are available on the official website of Rosfinmonitoring (<http://www.fedsfm.ru/>).

The list of sanctioned NGOs is published in the newspaper “Rossiyskaya Gazeta” and is available on the official website of Russian Ministry of Justice (<http://minjust.gov.ru/ru/activity/nko/unwanted>).

The full list of individuals on whom Russia has imposed a travel ban is not publicly available. However, the lists of some individuals who are subject to the travel ban may be available on the website of the Ministry of Foreign Affairs of the Russian Federation (<https://www.mid.ru/>).

The List of media platforms is available on the website of Roskomnadzor (<https://rkn.gov.ru/>).

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

No, there are no comprehensive sanctions or embargoes against countries or regions. We note, however, that in some cases sanctions imposed or implemented by Russia are fairly extensive. For example, the Ukrainian Sanctions relate both to Ukrainian individuals and entities and trading restrictions. Similarly, Russia has implemented a wide range of restrictive measures against North Korea in accordance with the UN Security Council Resolutions.

2.8 Does your jurisdiction maintain any other sanctions?

Import/export restrictions

In addition to the restrictions imposed on certain individuals and legal entities, Russia has imposed certain import restrictions on products from Albania, Australia, Canada, the EU, Iceland, Lichtenstein, Montenegro, Norway, Ukraine, the United Kingdom of Great Britain and Northern Ireland and the USA (pursuant to the Federal Law No. 127 dated 4 June 2018 “On measures (counter-measures) in response to inimical actions of the United States of America and other foreign countries”, as amended (the “Counter-Sanctions Law”), Decree of the President of the Russian Federation No. 560 dated 6 August 2014 “On application of certain special economic measures for the purposes of security of the Russian Federation”, as amended, and the Presidential Decree No. 592). In relation to Ukraine, certain restrictions are additionally imposed on the export of petroleum products.

The list of products from Albania, Australia, Canada, the EU, Iceland, Lichtenstein, Montenegro, Norway, Ukraine, the United Kingdom of Great Britain and Northern Ireland and USA that fall under the import ban is set out in the Governmental Resolution No. 778 dated 7 August 2014 (as amended). The above restrictions are extended until 31 December 2021.

Products from Ukraine, the import and/or export of which is restricted pursuant to the Presidential Decree No. 592, are listed in the Governmental Resolution No. 1716-83 dated 29 December 2018.

Similar import restrictions are imposed against Turkey (pursuant to Decree of the President of the Russian Federation No. 583 dated 28 November 2015 “On measures for national security of the Russian Federation and protection of Russian citizens against criminal and other wrongful actions and on application of special economic measures in relation to Republic of Turkey”, as amended).

Air travel ban

Air travel between Russia and Georgia is prohibited starting from 8 July 2019 by the Presidential Decree No. 287 dated 21 June 2019.

According to public statements of Russian authorities, in response to the air travel ban imposed by Ukraine on Russian airline companies, Russia imposed air travel restrictions in respect of Ukrainian airline companies in the same manner with effect from 25 October 2015.

2.9 What is the process for lifting sanctions?

Under the Sanctions Law, such restrictions may be lifted by the decision of the President of the Russian Federation pursuant to a proposal by the Federation Council of the Federal Assembly, State Duma of the Federal Assembly or the Government.

Pursuant to the Counter-Sanctions Law, the sanctions may be lifted by the Government upon the decision of the President.

We note that the decision on lifting the sanctions is generally based on reciprocity. Thus, in certain cases the Government may suggest lifting the counter-sanctions in relation to other jurisdictions if the sanctions imposed by such jurisdictions in relation to Russian individuals and entities are lifted.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

A special export control regime is introduced by the Federal Law No. 183-FZ dated 18 July 1999 “On export control” (as amended) in relation to products, information works services and IP rights that may be utilised for the creation of a weapon of mass destruction, vehicles for its delivery, other types of military equipment and/or may be used in preparation of execution of terrorist attacks (“Controlled Goods and Technologies”).

Export control in relation to military equipment and weapons is regulated by the Federal Law No. 114-FZ dated 19 July 1998 “On military-technical cooperation of the Russian Federation and foreign countries” (as amended).

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions’ sanctions or embargoes?

There are no such blocking statutes or any restrictions in place. Previously, draft bills on introducing criminal liability for compliance with sanctions imposed by other jurisdictions were discussed in public in 2018 and 2019. No such legislation has been approved by the Russian Federal Assembly so far.

However, Russian legislation contains a number of provisions on special measures relating to sanctions of foreign jurisdictions.

Media platforms

As described above, media platforms that are limiting access to information in the Russian Federation in connection with any sanctions imposed by foreign countries against Russia, Russian citizens or entities, may be blocked under Law No. 272.

Exclusive jurisdiction

In June 2020, Russian courts were granted exclusive jurisdiction over disputes involving sanctioned Russian entities. The law also allows commercial courts to issue anti-suit injunctions in relation to proceedings against sanctioned entities abroad.

Disclosure

The Russian Government is also authorised to adopt special regulations relating to mandatory disclosure of information. In 2019, the Government introduced certain exceptions relating to the disclosure of information (including by way of publishing a prospectus) by sanctioned persons and or persons that may fall under sanctions if such information is disclosed. Companies are now entitled to exclude from the information that is subject to disclosure, *inter alia*, information on management bodies, controlling and controlled persons, transactions made by such person or its controlled or controlling person, affiliates and related parties. Moreover, pursuant to Presidential Decree No. 388 dated 15 August 2019 (“Presidential Decree No. 388”), information on a Russian company’s shareholder that is subject to sanctions imposed by a foreign jurisdiction shall not be disclosed by the registrar (maintaining the shareholders register) to other shareholders at their request in case the company has notified the registrar of existence of such shareholder.

In addition to the above, access to certain information relating to sanctioned entities contained in the Unified State Register of Legal Entities is restricted pursuant to Resolution of Government of Russia No. 729 dated 6 June 2019. There are also similar exemptions on the disclosure of certain information regarding sanctioned entities in the Unified Federal Register of Information about Facts of Activities of Legal Entities.

Currency repatriation

Russian individuals or entities falling under sanctions of foreign jurisdictions shall be deemed as complying with their obligation on currency repatriation under Russian law, provided that such individuals or entities are included in the list maintained by the Federal Tax Service.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as “secondary sanctions”)?

No, there are no secondary sanctions.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction’s sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

Russian sanctions laws apply in the Russian Federation to Russian citizens, legal entities incorporated in Russia, foreign citizens and individuals with no citizenship residing in Russia, and foreign legal entities operating in Russia. We note that an administrative liability may be imposed on foreign citizens, individuals with no citizenship and foreign legal entities provided that a breach of sanctions laws took place in Russia. As for the criminal liability, as long as a foreign citizen or an individual with no citizenship commits a criminal offence against the interests of the Russian Federation, such individual may be held liable irrespective of whether such offence took place in Russia.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Ukrainian Sanctions. Under the Government Resolution No. 1300, all funds, securities and property of sanctioned persons in the Russian Federation shall be blocked (frozen). Such persons are not permitted to make any transfer of funds from the Russian Federation to another jurisdiction.

NGOs Sanctions. The financial institutions shall block (freeze) the transactions with funds and other property of listed NGOs.

UN Sanctions. Within the general procedure for AML and CFT control, funds or other property of persons listed in the Rosfinmonitoring’s lists, as well as entities owned or controlled by such persons (whether directly or indirectly) must be blocked (frozen) by financial institutions.

Sanctions against the U.S. citizens under Law No. 272. Pursuant to Law No. 272, U.S. citizens that are included in the list maintained by the Ministry of Foreign Affairs of Russia, are not permitted to engage in any transactions in respect of property located in Russia. Moreover, business operations of legal entities controlled by such individuals shall cease, and authorities of such individuals as members of governing bodies of any legal entity registered in Russia shall be terminated.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

The Russian Government may, upon a proposal from the Ministry of Finance, issue a licence in respect of certain operations that fall under Ukrainian Sanctions.

As for export control, any international trade activities in relation to the Controlled Goods and Technologies shall be licensed by Russian Federal Service for Technology and Export Control.

The Government is also authorised to issue a general licence for the export of certain categories of the Controlled Goods and Technologies to certain countries provided that the exporter is a Russian person that has adopted an internal export control programme and obtained a state accreditation certificate.

Moreover, the Russian Federal Service for Technology and Export Control is authorised to issue permits for the temporary export of the Controlled Goods and Technologies under certain conditions. As such, the applicant shall always have control over the exported goods and technologies and return such goods and technologies to Russia within the prescribed time limits. Permanent transfer of such goods and technologies to foreign parties is prohibited.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

In addition to general AML and CFT reporting requirements that are also applicable to the UN Sanctions, financial institutions are required to report information on the blocked transactions in respect of NGOs.

There are certain reporting requirements in relation to foreign sanctions. Pursuant to the Presidential Decree No. 388, in case a registrar of a Russian company is notified of a shareholder that is subject to foreign sanctions, the registrar shall provide the information on such shareholder to Central Bank of Russia within two business days.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

There are guidelines relating to compliance with AML and CFT Law. For example, the Central Bank of Russia issued internal audit guidelines for financial institutions (Letter No. 99-T dated 13 July 2005) and Rosfinmonitoring issued guidelines for blocking (freezing) of funds and assets in relation to non-financial organisations (Information Letter No. 60 dated 1 March 2019).

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Given that the UN Sanctions are implemented within the legislation on AML and CFT, criminal liability for violating the UN Sanctions may be imposed on a person who is at fault for violating the AML and CFT Law.

Management or involvement in operations of a sanctioned NGO in Russia may lead to criminal liability.

Violation of other sanctions does not, in and of itself, lead to criminal liability.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

Depending on the type of offence, the relevant government authority would be: (i) the Ministry of Internal Affairs of the Russian Federation; (ii) the Investigation Committee of the Russian Federation; or (iii) the Federal Security Service of the Russian Federation.

4.3 Is there both corporate and personal criminal liability?

No, only personal criminal liability may be imposed.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

For violating the AML and CFT Law, the maximum financial penalty is RUB 1,000,000 or the amount of the convicted person's salary or other income for up to five years.

The maximum financial penalty for management or involvement in operations of a sanctioned NGO is RUB 500,000 or the amount of the convicted person's salary or other income for up to three years.

4.5 Are there other potential consequences from a criminal law perspective?

For breach of AML and CFT Law, a person may be: convicted to mandatory work for a period of up to five years; limitation of freedom for a period of up to two years; deprivation of the right to hold certain offices or engage in certain activities for a period of up to five years; or may be imprisoned for up to seven years.

For management or involvement in operations of a sanctioned NGO, a person may be convicted to community service for up to 360 hours, mandatory work for up to five years, limitation of freedom for up to two years, deprivation of the right to hold certain offices or engage in certain activities for a period of up to 10 years, or may be imprisoned for up to six years.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

The Russian Federation Administrative Offences Code establishes administrative fines for the import of sanctioned products, sale of sanctioned products in Russia, and for operation of a listed NGO in Russia.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

The authorities responsible for investigating and enforcing administrative liability are: the Federal Customs Service; the Federal Service for Veterinary and Phytosanitary Control; the Federal Service for Control over Protection of the Consumers' Rights and Human Wellbeing; and the Federal Service for Technology and Export Control.

4.8 Is there both corporate and personal civil liability?

Yes, there is both corporate and personal civil liability.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

The penalty may amount to up to RUB 20,000 for officials and up to RUB 300,000 for legal entities.

4.10 Are there other potential consequences from a civil law perspective?

The imported products are to be confiscated and destroyed.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

All regulations relating to administrative liability are publicly available. The resolutions by the competent authorities are available to the parties involved. However, there is no detailed regulation of the assessment of penalties.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

In the case that the relevant authority has issued a resolution imposing an administrative liability, such resolution may be challenged in court. We are aware of cases where companies have successfully challenged penalty assessments and were released from any liability.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal and administrative enforcement in relation to sanctions may take place only at the national level.

4.14 What is the statute of limitations for economic sanctions violations?

The statute of limitations for criminal liability depends on the gravity of the offence which is determined based on factual circumstances, and may be from two years (for minor crimes) to 10 years (for especially grave crimes).

The statute of limitations for administrative offences depending on the type of offence may be from two months to two years.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

The State Duma of the Federal Assembly of the Russian Federation is currently considering two draft bills introducing sanctions-related amendments. Pursuant to one of the draft bills, the list of sanctioned persons under Law No. 272 may include not only U.S. citizens but also citizens of other foreign countries. The second draft bill, if passed, may prohibit the provision of information by Russian banks at the request of state authorities of listed countries unless such provision of information is made in compliance with Russian legislation.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Russian legislation related to sanctions is available in Russian at <https://www.pravo.gov.ru/>. Only a limited number of regulations are available in English on the websites of governmental authorities or commercial databases; however, such English translations are not official.



Oleg Isaev is a partner in the Corporate practice and advises clients on a variety of domestic and cross-border transactions, focusing primarily in the areas of mergers and acquisitions, private equity and general corporate matters. He has had extensive experience in advising clients on oil and gas legislation, corporate financing transactions, antimonopoly and compliance issues. In addition, Oleg also advises clients on the placement of securities, financing, currency regulation and currency control issues, as well as various commercial contracts.

Rybalkin, Gortsunyan & Partners

2 Tsvetnoy Boulevard, Entrance C, 5th Floor
127051, Moscow
Russia

Tel: +7 495 139 65 00

Email: oisaev@rgp.legal

URL: www.rgp.legal



Anastasia Konstantinova is a counsel in our Dispute Resolution practice. She specialises in litigation issues, corporate law and competition. She also has experience in advising clients on mergers and acquisitions, corporate restructurings, conducting due diligence of Russian companies in the oil and gas, pharmaceutical and real estate sectors, as well as participating in internal investigations.

Rybalkin, Gortsunyan & Partners

2 Tsvetnoy Boulevard, Entrance C, 5th Floor
127051, Moscow
Russia

Tel: +7 495 139 65 00

Email: akonstantinova@rgp.legal

URL: www.rgp.legal



Marina Abazyan is a corporate associate at RGP. Marina focuses her practice on mergers and acquisitions, capital markets transactions, corporate governance and general corporate law matters.

Rybalkin, Gortsunyan & Partners

2 Tsvetnoy Boulevard, Entrance C, 5th Floor
127051, Moscow
Russia

Tel: +7 495 139 65 00

Email: mabazyan@rgp.legal

URL: www.rgp.legal

Rybalkin, Gortsunyan & Partners (RGP) is a fast-paced law firm of the next generation, combining a leading Russian practice focusing on international dispute resolution and a high-end corporate practice servicing complex transactions and projects.

We support clients from all over the world in their business dealings in our key practice areas involving Russia and CIS countries. In addition, our firm offers unparalleled expertise in foreign legal matters to Russian companies with significant international presence.

We are a cohesive team of seasoned professionals with a background in leading international law firms.

Our lawyers have worked on the largest corporate deals, investigations and disputes in the history of modern Russia and represented Russian companies in over 170 jurisdictions worldwide.

www.rgp.legal

**RYBALKIN
GORTSUNYAN
PARTNERS**

Sweden

Advokatfirman Vinge KB



Anders Leissner



Tove Lövgren Frisk

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

Sweden does not issue any sanctions of its own. Sanctions that apply in Sweden are sanctions decided by the United Nations or the European Union. To the extent such sanctions are not automatically binding in Sweden because of a treaty or public international law principles, such sanctions are enacted by way of a legislative process provided for in §3 of the Act (1996:95) on certain international sanctions (hereinafter the Swedish Sanctions Act) pursuant to which an Ordinance is issued.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

There is no general sanctions authority in Sweden. Instead, several government agencies are involved in the administration and enforcement of sanctions.

The Inspectorate of Strategic Products (Sw: *Inspektionen för strategiska produkter*) deals with issues pertaining to weapon embargoes, dual-use products, prohibitions regarding equipment used for internal repression and the release of frozen assets.

The National Board of Trade Sweden (Sw: *Kommerskollegium*) deals with licence requirements pertaining to sanctions and export of products and services.

In addition, various agencies, such as the Swedish Financial Supervisory Authority (Sw: *Finansinspektionen*) and the Swedish Customs, supervise and enforce compliance within their areas of responsibility.

The respective agency's responsibilities are often described in the relevant Ordinance pertaining to the particular sanctions (although an Ordinance is not always issued, see question 1.1). For instance, following the Ordinance that the Swedish government issued implementing the sanctions which were imposed against Russia by way of Council Decision 2014/512, five different agencies are charged to perform various tasks.

Criminal enforcement is entrusted to the prosecutor-general, which is why the Swedish Prosecution Authority has an important role regarding the enforcement of sanctions and which also can involve The Swedish Security Services (Sw: *Säkerhetspolisen*).

Finally, the Swedish foreign ministry has the overall responsibility for "coordinating Sweden's sanctions policy" as expressed on their website.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

Sanctions is an area under constant development and numerous changes have been made in respect of the European Union sanctions regime during the past year. One of the more notable recent changes is the imposition of a European Union global human rights sanctions regime on 7 December 2020.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Sanctions in Sweden (i.e. sanctions imposed by the European Union and United Nations) are imposed pursuant to the Swedish Sanctions Act.

In addition, the European Union has the power to impose sanctions against third countries which have direct binding effect on all Member States. The European Union's competence in this respect derives from the European Union treaties (see TEU Article 29 and TFEU Article 215 regarding restrictive measures, as well as TEU Articles 21–46 regarding the European Union's joint foreign and security policy).

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Sweden's policy is to implement sanctions which have been decided or recommended by the United Nations Security Council in accordance with the Charter of the United Nations, see §1 of The Swedish Sanctions Act.

In practice, United Nations sanctions are generally imposed within the European Union – and consequently Sweden – through instruments issued by the European Union (see question 2.3). There are no significant ways in which Sweden fails to implement United Nations sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

Sweden is a member of the European Union.

- (a) The Council of the European Union issues restrictive measures through CFSP Council decisions under Article 29 of the TEU. Measures such as arms embargoes or restrictions on admission are implemented by the European Union Member States, meaning that the Swedish government will make a legislative proposal to the parliament for approval of an Ordinance in line with the process described in the Swedish Sanctions Act. Other measures, including measures freezing funds and export bans, are generally implemented by the Council, acting by qualified majority on a joint proposal from the High Representative of the Union for Foreign Affairs and Security Policy and the Commission, through a regulation (Article 215 of the TFEU). Such regulations are binding and directly applicable on all Member States.
- (b) No, there are none.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Sweden does not administer a sanctions list of its own. Instead, the Swedish government refers to the consolidated sanctions lists provided by the United Nations and European Union.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

A challenge of a listing by the European Union can be made before a Swedish court. It can also be made by way of a challenge before the General Court of the European Union or by way of submitting a de-listing request to the General Secretariat of the Council of the European Union.

United Nations sanctions can be challenged by way of a de-listing request to the United Nations organisation. In the event the listing is related to the ISIL (Da'esh) and Al-Qaida sanctions list, the request can also be sent to the United Nations ombudsman.

There is no formal procedure in place imposing obligations on the Swedish government to assist Swedish citizens in challenging sanctions listings, although there are examples where such assistance has been provided.

2.6 How does the public access those lists?

Sanctions lists provided by the European Union and United Nations are publicly available on the internet. The United Nations Security Council's consolidated list can be found on the UN website. A presentation of the sanctions at European Union level can be accessed via the European Union Sanctions Map.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

As mentioned under question 1.1, only sanctions imposed by the United Nations and the European Union apply in Sweden. Following those sanctions regimes, the most comprehensive sanction programmes in Sweden are against Crimea, North Korea and Syria (at the time of writing).

2.8 Does your jurisdiction maintain any other sanctions?

Following the United Nations and European Union sanction regimes, Sweden has 32 sanctions programmes in place as of May 2021.

2.9 What is the process for lifting sanctions?

There is no process in Sweden for revoking or lifting sanctions imposed by the European Union or United Nations since the decision to lift sanctions rests with the legal or administrative authority which first enacted the sanction. Regarding the possibilities for a listed entity to remove a particular listing, please refer to the answer under question 2.5 above.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes. Export control matters in Sweden are governed by Council Regulation 428/2009 and associated legal instruments. As of May 2021, the regulation is in the process of being updated/replaced.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Yes. European Union's Blocking Statute, Council Regulation (EC) No 2271/96, apply in Sweden.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

No, it does not.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

Violations committed within the Swedish territory, or by a Swedish citizen abroad, is subject to the Swedish Sanctions Act. The European Union sanctions apply:

- within EU territory, including its airspace;
- to EU nationals, whether or not they are in the EU;
- to companies and organisations incorporated under the law of a Member State, whether or not they are in the EU (including branches of EU companies in third countries);
- to any business carried out in whole or in part within the European Union; and
- on board aircrafts or vessels under the jurisdiction of a Member State.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

To what extent parties are required to block funds or other property in relation to sanctions prohibitions will depend on the relevant sanctions regime. To this end, asset freeze is a common feature in sanctions applying in Sweden, e.g., sanctions issued by the European Union and the United Nations. When freezing measures apply, no funds or economic resources may be made available to the listed individual or entity.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes, provided such remedy is possible according to the text of the relevant sanctions regime. Applications regarding export licences and exceptions from asset freeze provisions are made to the National Board of Trade Sweden. Applications regarding the release of frozen funds shall be made to the Inspectorate of Strategic Products.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

According to Swedish law, there are no general reporting requirements although a licence (see question 3.3) may come with such a requirement. However, European Union sanctions regulations typically contain a general, although vague, obligation requiring all natural or legal persons, entities and bodies subject to the regulations to report any information which would “facilitate compliance” with financial sanctions.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

The Swedish government has not provided any sanctions compliance guidance such as the guidance provided by OFAC and OFSI. The European Union has, however, provided some guidance which is available on the European Commission’s website (to which the Swedish government’s website refer).

Further, the European Union has a due diligence helpdesk for small- and medium-sized corporations dealing with Iran.

Notably, sanctions screening of individuals against sanction lists that are not legally binding in Sweden, for instance the SDN list, requires a permit from the Swedish Authority for Privacy Protection for GDPR reasons. Although the authority seems to generally grant such permits, in particular, to financial institutions which are subject to AML requirements, the Swedish permit requirement makes compliance increasingly difficult.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes, there are.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The Swedish Prosecution Authority is responsible for investigating and prosecuting criminal economic sanctions offences.

4.3 Is there both corporate and personal criminal liability?

Natural persons are exposed to criminal liability pursuant to the Swedish Sanctions Act §8. Natural persons can, however, only be prosecuted after a decision by the government or the prosecutor-general.

According to Swedish law, legal persons cannot be subject to criminal liability as such, i.e. a legal person cannot commit a crime. However, if a natural person has committed an offence in the exercise of a company’s business activities, the company may be subject to a corporate fine, constituting a so-called “special legal consequence of offence” (Sw. *särskild rättsverkan av brott*), according to the Swedish Penal Code Chapter 36 §§ 7-10a. These rules do not only apply in relation to sanction breaches, but to all criminal activities committed within a corporations’ business activities.

The determining factor in deciding the level of the corporate fine is the offence itself or the severity of the offence, i.e. how serious the offence is and the extent to which criticism can be levelled against the company. After 1 January 2020, the financial situation of the company may also be taken into account in setting the level of the corporate fine where the situation involves particularly serious offences (“increased corporate fines”).

The rules regarding increased corporate fines only apply to offences committed after 1 January 2020. The maximum level of the corporate fine is SEK 500,000,000 (SEK 10,000,000 for offences committed prior to 1 January 2020).

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

Legal entities (including sole proprietorship) may be subject to a corporate fine amounting to a maximum of SEK 500,000,000 (see further question 4.3 above).

The maximum financial criminal liability for individuals is SEK 150,000.

4.5 Are there other potential consequences from a criminal law perspective?

Pursuant to §8 of the Swedish Sanctions Act, a breach of sanction laws can entail a prison sentence of a maximum of two years, or if the breach is gross, four years. If the breach is caused by gross negligence, the prison sentence is a maximum of six months.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

There is no particular regime for civil penalties. However, breach of sanctions undertakings in contracts may of course lead to an obligation to pay damages depending on the contract

terms. Also, note that legal persons may be subject to corporate fines constituting a special legal consequence of offence (see question 4.3 above).

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

This is not applicable since there is no civil liability (however, see question 4.3 above on corporate fines constituting a special legal consequence of offence).

4.8 Is there both corporate and personal civil liability?

This is not applicable since there is no civil liability (however, see question 4.3 above on corporate fines constituting a special legal consequence of offence).

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

This is not applicable since there is no civil liability (however, see question 4.3 above on corporate fines constituting a special legal consequence of offence).

4.10 Are there other potential consequences from a civil law perspective?

No, there are not.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

This is not applicable.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Appeal of a criminal conviction decided by the District Court (i.e. generally the court of first instance) is made pursuant to the process described in Chapter 49 §1 and Chapter 51 of the Swedish Code of Judicial Procedure. The appeal is made to the District Court and should be made within three weeks. After having verified fulfilment of certain formal requirements, the District Court passes on the appeal to the Court of Appeal which try the case. Appeal of a judgment by the Court of Appeal to the Supreme Court will require a review permit.

Appeal of a corporate fine (see question 4.3) follows the same procedure; however, a permit is required from the Court of Appeal in the event no individual has been convicted in relation to the fine.

There is no established practice regarding the level of penalties for sanction breaches in Sweden. Likewise, there are few court decisions pertaining to sanction breaches. At least one decision suggests that sanction breaches generally should be considered as relatively severe crimes (see RH 1998:18).

Penalty levels in Sweden generally have historically been relatively low compared to, e.g., the United States and hence there have previously not been any obvious financial incentive for corporations to challenge penalty assessments. However, this may now change considering the recent increase in the maximum level of corporate fines that may be imposed as of 1 January 2021.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

This is at national level only.

4.14 What is the statute of limitations for economic sanctions violations?

The statute of limitations for economic sanctions violations is 10 years.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

There are none.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

The main information source about sanctions in Sweden is the Swedish government website (English version), <https://www.government.se/government-policy/foreign-and-security-policy/international-sanctions/>.

The English version of the website of the Inspectorate of Strategic Products is <https://isp.se/eng>. Information about sanctions including applications forms for the release of frozen funds is, however, only available on the Swedish version of the website.

The English version of the website of the National Board of Trade Sweden is <https://www.kommerskollegium.se/en/>. Again, however, information about sanctions only seem to be available on the Swedish version of the website.

Information from the United Nations regarding how to submit a de-listing request can be found here: <https://www.un.org/securitycouncil/sanctions/delisting>.

The European Union helpdesk for small- and medium-sized corporations dealing with Iran can be found here: <https://www.sanctions-helpdesk.eu/>.

Information about submitting a request to the Council to lift restrictive measures by the European Union can be found here: <https://www.consilium.europa.eu/en/policies/sanctions/adoption-review-procedure/>.



Anders Leissner has worked at a leading international maritime insurance company for more than 20 years, 11 years of which has been spent as General Counsel. This has given him broad and practical experience from a number of practice areas ranging from corporate governance to dispute resolution both from a Swedish and international perspective, as well as general risk management issues. Anders has significant experience in relation to sanction issues, in particular, as to how the sanction legislation in the United States affects companies within the EU, which has included both risk assessments, contract issues and management of incidents in co-operation with Swedish and foreign public authorities. He has also participated in several international industrial organisations that have prepared sanction clauses and other contractual terms and conditions for the shipping and insurance sector.

Advokatfirman Vinge KB
 Nordstadstorget 6, Box 11025
 SE-404 21 Göteborg
 Sweden

Tel: +46 10 614 15 20 / +46 72 179 15 20
 Email: anders.leissner@vinge.se
 URL: www.vinge.se



Tove Lövgren Frisk has a background in M&A but has worked solely with corporate crime and compliance-related matters during the last couple of years. Tove has advised clients in relation to anti-corruption, money laundering, sanctions, export control and corporate crime. Tove has also advised national and international companies on adopting, implementing and reviewing anti-corruption compliance programmes, as well as conducted forensic investigations on behalf of domestic and international companies in order to address suspicions of fraud, bribery and corrupt practises. In addition, Tove is a writer in the area of Anti-Corruption and Corporate Crime.

Advokatfirman Vinge KB
 Smålandsgatan 20, Box 1703
 111 87 Stockholm
 Sweden

Tel: +46 10 614 34 90 / +46 76 887 34 90
 Email: tove.lovgrenfrisk@vinge.se
 URL: www.vinge.se

Advokatfirman Vinge is one of Sweden's leading independent commercial law firms with approximately 450 employees. We continuously receive top ranking by institutes such as *Mergermarket*, *Chambers and Partners*, *The Legal 500* and *IFLR*. Vinge's business concept is to be the leading Swedish business law partner, contributing to the success of its clients through its level of commitment, simplicity in approach and focus on results.

We have established a unique level of competence and provide a full business law service. In particular, Vinge has in-depth expertise within the areas of International Trade, Corporate Crime and Compliance.

We are privileged to work with a large number of major international public and private companies, financial institutions and governments on some of the most complex and challenging mandates and transactions in the Nordic region.

www.vinge.se

VINGE

Switzerland



Claudio Bazzani



Reto Ferrari-Visca

Homburger

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

The Swiss sanctions regime is governed by the Federal Act on the Implementation of International Sanctions, also known as the Embargo Act (EmbA).

The EmbA is a framework law that authorises the Federal Council to impose non-military measures in order to implement sanctions that have been imposed by the United Nations, the Organisation for Security and Cooperation in Europe (OSCE) or by Switzerland's most significant trading partners (e.g., the European Union) for the enforcement of international law, in particular, of human rights.

Possible sanctions under the EmbA are direct or indirect restrictions of transactions involving goods and services, payment and capital transfers, the movement of persons, scientific, technological and cultural exchange, as well as prohibitions, licensing and reporting obligations and other restrictions of rights.

If sanctions exclusively relate to war materiel, military equipment and related technology, the Federal Act on War Material (War Material Act, WMA) and the Federal Act on the Control of Dual-Use Goods, Specific Military Goods and Strategic Goods (Goods Control Act, GCA) are applicable.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The State Secretariat for Economic Affairs (SECO) is the main authority responsible for monitoring and implementing sanctions. For specific sanction types, other agencies may be responsible (e.g., the State Secretariat for Migration for travel bans, the Federal Office of Civil Aviation for air traffic restrictions or the Federal Customs Administration for border controls).

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

There have been no significant changes or developments impacting Switzerland's sanctions regime over the past 12 months.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The Federal Council is responsible for implementing sanctions imposed by international organisations (e.g., United Nations, OSCE and the European Union).

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Yes. Between 1990 and 2002, Switzerland participated autonomously in non-military sanctions imposed by the United Nations. Since 2002, when Switzerland became a Member State of the United Nations, Switzerland has been required to implement non-military sanctions of the United Nations.

Once the United Nations has established a sanctions regime under Chapter VII of the United Nations Charter, the Federal Council will issue an ordinance implementing the non-military sanctions imposed by the United Nations. Depending on the circumstances, the implementation usually takes between a few days and several weeks.

Switzerland has currently implemented all relevant United Nations sanctions.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

The Federal Council is authorised to implement sanctions issued by the OSCE (of which Switzerland is a Member State) and the European Union.

Currently, there are no significant ways in which Switzerland fails to implement sanctions of the OSCE or the European Union.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Yes. The lists of sanctioned individuals and entities are maintained and updated by the SECO (see the answer to question

2.6). However, the decision of whether individuals and entities will be added to or removed from a sanctions list lies with the Federal Council (see the answer to question 2.1). In general, the sanctions lists will be updated in accordance with the sanctions lists issued by the United Nations.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Individuals or entities may challenge their addition to a sanctions list. In practice, however, the responsible agencies and courts reject the delisting as long as the individual or entity concerned is mentioned on sanctions lists issued by the United Nations.

2.6 How does the public access those lists?

The lists of sanctioned individuals and entities can be found on the website of the SECO: https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen.html.

The SECO also provides an online tool in order to search for sanctioned individuals and entities. The search tool, including a user guide, can be found on the following website: https://www.seco.admin.ch/seco/de/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen/suche_sanktionsadressaten.html.

In addition, updates regarding sanctioned individuals and entities can be received via the newsletter service of the Swiss government and the Swiss Financial Market Supervisory Authority FINMA (FINMA).

Finally, the sanctions lists are published in the Systematic Compilation of Federal Legislation.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

Comprehensive sanctions have become less important due to their negative effects on the civilian population. Nowadays, the focus is on so-called smart sanctions limited to the political and military leadership or strategically important goods.

Switzerland has imposed sanctions on different countries, including but not limited to Belarus, Lebanon, Iraq, Iran, Myanmar, North Korea, Venezuela and several African countries (e.g., Zimbabwe).

Whereas some of the sanctions are targeted at the political and military leadership and affiliated individuals and entities of these countries (e.g., asset blocks and travel bans), other sanctions relate to specific goods (e.g., armaments, goods for repression or surveillance, luxury goods).

2.8 Does your jurisdiction maintain any other sanctions?

Yes. Switzerland has also imposed sanctions on individuals and organisations with connections to Usama bin Laden, the “Al-Qaida” group and the Taliban, as well as on specific individuals that were involved in the attack on Rafik Hariri.

In addition, Switzerland has implemented the Kimberly Process (based on the United Nations General Assembly Resolution 55/56 and United Nations Security Council Resolution 1459) by issuing the ordinance on the international trade of rough diamonds in

order to prevent so-called blood or conflict diamonds from entering the markets.

2.9 What is the process for lifting sanctions?

The Federal Council may lift sanctions by abolishing or amending the ordinance that imposed the sanctions.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes. For war materiel, military equipment and related technology, as well as for goods that are usable for both civilian and military purposes (dual-use goods), the WMA and the GCA, respectively, are applicable. The Swiss export control regime implements requirements from international treaties and export control regimes (e.g., Arms Trade Treaty, Australia Group, Biological Weapons Convention, Chemical Weapons Convention, Missile Technology Control Regime, Nuclear Suppliers Group, Treaty on the Non-Proliferation of Nuclear Weapons, Wassenaar Arrangement).

Both acts stipulate a licensing regime with special requirements. Materiel and technology subject to the WMA may not, *inter alia*, be produced, traded with, brokered, imported, exported or transited unless the applicable licence has been granted. In addition, the WMA prohibits the development, production and trade of weapons of mass destruction (nuclear, biological and chemical weapons), anti-personnel mines and cluster munition, as well as the direct and indirect financing of such activities.

The export of goods that are subject to the GCA is also restricted unless the applicable licence has been granted. In addition, each export must be reported.

In general, the SECO is the responsible licensing and reporting authority. For licences regarding nuclear goods, however, the Swiss Federal Office of Energy is responsible.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Switzerland does not have restrictions in place that prohibit adherence to other jurisdictions' sanctions or embargoes, with the exception of blocking statutes and secrecy and data protection regulations that may restrict compliance with foreign reporting obligations related to sanctions.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as “secondary sanctions”)?

Currently, Switzerland does not have a regime for so-called “secondary sanctions”.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

There are both sanctions against specific individuals and entities,

as well as against countries, in place (see the answers to questions 2.7 and 2.8). If the sanction relates to specific individuals and entities, no transactions may be made to them or to entities controlled by them irrespective of their nationality or current stay or residence.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Yes. Most sanctions regimes require that assets of sanctioned individuals or entities must be blocked.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes. The Federal Council may stipulate exceptions in order to support humanitarian activities or to safeguard Swiss interests, in particular for the provision of food supplies, medicines and therapeutic products for humanitarian purposes. In addition, the Federal Council may delegate the authorisation to grant an exception to the SECO or another agency.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Yes. Most sanctions regimes require individuals or institutions that hold or manage assets of sanctioned individuals or entities, or have knowledge of the existence of such assets, to inform the relevant supervisory authority. The report must include the names of the beneficiaries as well as the specification and value of the assets.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

The SECO has published best practices for an Internal Control Program for Export Controls (ICP) in English and a fact sheet for the ICP. According to these best practices, an ICP shall include the following elements:

1. management commitment and policy statement regarding export controls and sanctions;
2. definition of roles and responsibilities to guarantee compliance with export controls and sanctions;
3. compliance with licensing requirements (i.e., classification of goods, software and technology to be exported);
4. “know your customer” as well as checks of end-user and end-use;
5. training and information of employees involved; and
6. internal audits.

In addition, the SECO has published a red flag checklist for exports and a questionnaire for qualifying products as war material, as well as a non-binding overview of the export control regulations (“export control in a nutshell”).

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Both intentional and negligent violations constitute criminal offences. A breach of sanctions may result in imprisonment for

up to five years, which may be combined with a fine of up to CHF 1 million.

Furthermore, any refusal to cooperate with the supervisory authorities and other misdemeanours may lead to a fine of up to CHF 100,000.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The supervisory authority, which is in general the SECO, is responsible for investigating and prosecuting economic sanctions offences. In case of a serious violation, the responsible supervisory authority may ask the Office of the Attorney General of Switzerland to initiate an investigation.

4.3 Is there both corporate and personal criminal liability?

Primarily, the individual committing the violation is personally liable. In addition, board members, directors, employers, delegators or principals who intentionally or negligently fail to prevent a breach committed by a subordinate or employee may be held liable. Additionally, there is corporate liability if it is not possible to attribute the violation to a specific individual due to the inadequate organisation of the corporation.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

The maximum financial penalty is CHF 1 million for serious sanctions violations and CHF 100,000 for the refusal to cooperate with the supervisory authorities and other misdemeanours.

The GCA stipulates a maximum financial penalty of CHF 5 million and the WMA stipulates a monetary penalty with a maximum of CHF 540,000.

4.5 Are there other potential consequences from a criminal law perspective?

Yes. Assets acquired and income generated by violating sanctions provisions may be confiscated.

The SECO or other competent agencies may suspend or revoke authorisations they have granted due to sanctions law violations. Furthermore, the depth and frequency of governmental audits may increase.

Additionally, potential consequences can be negative effects on the reputation of the corporations and individuals involved in the sanctions violation. They may also be excluded from public tenders due to the sanctions violation and contracts may include a termination clause for serious violations of laws, including sanctions laws. Finally, FINMA may initiate enforcement proceedings against supervised entities and individuals that have been involved in (alleged) sanctions violations.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

No. There are currently no civil penalties for violating economic sanctions laws and/or regulations in Switzerland.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

Not applicable (see the answer to question 4.6).

4.8 Is there both corporate and personal civil liability?

Not applicable (see the answer to question 4.6).

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

Not applicable (see the answer to question 4.6).

4.10 Are there other potential consequences from a civil law perspective?

Not applicable (see the answer to question 4.6).

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

Not applicable (see the answer to question 4.6).

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Not applicable (see the answer to question 4.6).

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal enforcement is only at the national level. However, the responsible national supervisory authorities may involve the

cantonal or communal police as well as investigating officers from the Federal Customs Administration for assistance in connection with inspections, searches and seizures.

4.14 What is the statute of limitations for economic sanctions violations?

For serious economic sanctions violations, the statute of limitations is 15 years. For other economic sanctions violations, the statute of limitations is seven years. For refusal to cooperate with the supervisory authorities and other misdemeanours, the statute of limitations is five years.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

Currently, there are no sanctions-related measures proposed or under consideration in Switzerland.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

The SECO maintains a public website with information and guidance on export controls and sanctions in German, French and Italian. Some of the information is also available in English. The link to the website in English is as follows: https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen.html.



Claudio Bazzani is a partner and co-head of Homburger's white-collar/investigations working group and the litigation and arbitration practice. He specialises in large-scale internal and regulatory investigations and advises corporate clients in compliance matters. He represents clients in investigations by Swiss and foreign authorities, and in domestic and international litigation and arbitration proceedings. Claudio Bazzani has more than 10 years of experience in internal and regulatory investigations and compliance matters. He regularly speaks at conferences and publishes on topics related to his area of expertise.

Homburger AG

Prime Tower, Hardstrasse 201
8005 Zurich
Switzerland

Tel: +41 43 222 16 02

Email: claudio.bazzani@homburger.ch

URL: www.homburger.ch



Reto Ferrari-Visca is an associate of Homburger's white-collar/investigations working group and the litigation and arbitration practice. He specialises in domestic and international litigation and administrative proceedings. He has experience in internal and regulatory investigations and advises corporate clients in regulatory and compliance matters. His practice also focuses on privacy and data protection law and he regularly advises clients on cross-border privacy and data protection issues.

Homburger AG

Prime Tower, Hardstrasse 201
8005 Zurich
Switzerland

Tel: +41 43 222 12 50

Email: reto.ferrari-visca@homburger.ch

URL: www.homburger.ch

Homburger is a full-service corporate law firm and advises and represents companies and executives in transactions as well as in complex cases, both in the domestic and the international context.

We offer our clients comprehensive legal advice, provide support in negotiations, and represent them before courts, arbitral tribunals, agencies, and in administrative proceedings. In doing so, we place great value not only on the identification of sustainable solutions to complex legal issues, but also on the achievement of our clients' individual commercial goals. We work closely with leading law firms, enabling us to provide our clients with optimal solutions, regardless of where their business activities take place. We are organised around our main areas of practice: capital markets; corporate/M&A (including private equity); financial services (incl. insurance); litigation/arbitration; tax; intellectual property/technology; and competition/regulatory. In addition, we focus on white-collar/investigations, employment/pensions, private clients, real estate, and restructuring/insolvency.

www.homburger.ch

Homburger

United Arab Emirates

BSA Ahmad Bin Hezeem & Associates LLP



Rima Mrad



Tala Azar

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

The United Arab Emirates (“UAE”) has a complex sanctions regime based on a variety of sources. Sanctions are based on diverse interests, including political, economic, and national security interests. Due to the rapidly changing nature of such interests, sanctions are susceptible to significant and constant changes.

Sanctions in the UAE are usually imposed at a federal level, through a variety of methods, including, by way of example:

- a. *Adding sanctioned persons to local lists and the United Nations (“UN”) sanctions list:* This is effected by issuing local terrorism lists (“**Local Lists**”) and implementing the sanctions passed by the UN Sanctions Committee (“**Sanctions List**”) pursuant to Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (“**AMLCFT Law**”), Cabinet Decision No. 10 of 2019 concerning the Implementing Regulation of the AMLCFT Law (“**AMLCFT Implementation Regulation**”), the recent Cabinet Decision No. 74 of 2020 concerning the UAE List of Terrorists and the Implementation of UN Security Council Decisions Relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of Mass Destruction, and the Relevant Resolutions (“**New Sanctions Regulations**”) and Federal Law No. 7 of 2014 on Combating Terrorism Offences. Guidance was issued on targeted financial sanctions by the Executive Office of the Committee for Goods and Materials subject to Import and Export Control (“**Office**”) on 6 May 2021 further setting out the implementation of the New Sanctions Regulations (the “**New SR Guidance**”).
- b. *Issuing specific laws addressing specific sanctions against a country or persons:* This is not currently in effect except with regards to laws providing the legal basis for sanctions lists as mentioned above. The last example of a law addressing specific sanctions against a country or its nationals was Federal Law No. 15 of 1972 concerning the Boycott of Israel (“**Israel Boycott Law**”), which was repealed by virtue of Federal Decree Law No. 4 of 2020.
- c. *Others:* Where sanctions are issued by inter-governmental organisations (“**IGOs**”) of which the UAE is a member, these sanctions are implemented by adding the sanctioned persons to the Sanctions List (as stated above) and/or issuing internal circulars to the relevant governmental entities.

With respect to trade specifically, the Ministry of Economy is responsible for regulating trade restrictions and sanctions; for instance, it recommended issuance of Federal Law No. 13 of 2007 concerning the Commodities subject to the Monitoring of Imports and Exports (“**Commodities Law**”), which, among others, prohibits the export or re-export of strategic goods and dual-use items without a special licence.

In addition to the above methods, multiple laws and regulations are regularly issued to additionally impose restrictions and require that persons in the UAE, particularly in financial and regulated industries, undertake implementation measures such as reporting requirements and client due diligence, in order to ensure compliance with UAE and international sanctions such as those of the UN, Office of Foreign Assets Control (“**OFAC**”) and the European Union (“**EU**”), as applicable. As a member of the UN, the UAE is required to comply with all sanctions passed by the UN Security Council.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The UAE administers sanctions through different governmental entities, depending on the implementation measures required for the imposition of the relevant sanctions. Two governmental authorities often used in the implementation of sanctions are the Office and UAE central bank (“**Central Bank**”):

1. *Office:* The Commodities Law authorises the restriction or ban on import, export or re-export of goods deemed as a threat to the UAE’s foreign policy. As the UAE authority responsible for implementing the AMLCFT, the Office articulates obligations in the New SR Guidance having the force of law.
2. *Central Bank:* The Central Bank is a fundamental authority that handles the compliance with sanctions as applicable to financial institutions (“**FIs**”). Its authorities include the prohibition of transactions with Designated Persons and the freezing of funds of Designated Persons.
3. *Customs authorities:* To the extent where they are able and empowered to confiscate and freeze any shipment that is in breach of any applicable sanctions in the UAE.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

There have been certain significant changes and developments impacting the UAE’s sanctions regime over the past 12 months.

Notably, from a legislative framework perspective, the UAE’s previous sanctions regulations and implementation regulations

were abrogated, and new such legislation was issued. Also, the Israel Boycott Law was repealed.

From a substantial perspective, among other changes, compliance obligations and required steps by UAE persons have increased, as illustrated in the New SR Guidance.

From a more practical perspective, sanctions against Israel and Qatar were repealed.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

The Supreme Council for National Security, the UAE Cabinet and the UN Security Council are the ultimate entities responsible for imposing sanctions. The Supreme Council for National Security proposes sanctions both internally and to the UN Sanctions Committee pursuant to Article 2 of the New Sanctions Regulations. The UAE Cabinet and the UN Security Council impose sanctions by issuing the Local List and Sanctions List, respectively. The Office, with implementation powers: (1) circulates the names of the Designated Persons to supervisory authorities, security agencies, FIs and DNFBBs; and (2) makes available the updated Sanctions List and Local List to the public by publishing the same on its website. It also issued guidance on implementation regulations of the New Sanctions Regulations, which include additional obligations on all UAE persons.

As illustrated under our answer to question 1.1 above, sanctions have also in the past been imposed by way of the issuance of Federal Laws and Cabinet Decisions, however, this occurs less often.

The UAE may, in certain circumstances, implement sanctions issued by IGOs (other than the UN) of which it is a member and would update its sanctions list to that effect.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

The UAE implements UN sanctions issued by the UN Sanctions Committee. The AMLCFT Law requires “[p]rompt application of the directives when issued by the competent authorities in the state for implementing the decisions by the UNSC under Ch. 7 of UN Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of weapons of mass destruction, and other directives”.

The New Sanctions Regulations and New SR Guidance set out the implementation framework of the Sanctions List, including the coordination and implementation role of the Office. The Office imposes direct responsibilities on and accords power to the supervisory authorities of FIs and DNFBBs to implement the Sanctions List. Moreover, the New SR Guidance imposes obligations on FIs and DNFBBs, and all other natural and legal persons in the UAE, to implement the Sanctions List. DNFBBs consist of anyone conducting one or more of the commercial or professional activities listed in the implementing regulation of the AMLCFT Law, which include certain real estate brokers and agents, merchants of precious metals and precious stones, lawyers, and providers of corporate services.

Pursuant to the New SR Guidance, the Office has imposed a number of obligations on all persons in the UAE (legal and natural), including DNFBBs and FIs, to ensure implementation of UN Sanctions:

1. All such persons must register with the Office, and the Office shall inform them, via automated email notifications, of any changes to the Sanctions List.

2. All such persons are required to have screening measures in place which must be undertaken on a daily basis as per the requirements in the New SR Guidance.
3. Application of targeted financial sanctions (“TFS”), including by freezing funds, and not making funds available.
4. Notification requirements.

DNFBBs and FIs are subject to additional obligations as set out in the New SR Guidance. These include setting internal controls and procedures to ensure compliance with the New Sanctions Regulations, as well as policies and procedures to prohibit staff from informing any customer or third party of impending freezing action.

It is worth noting that in certain cases, sanctions imposed by the UN may have already been implemented by the UAE on other grounds and included in Local Lists, e.g., as a result of its membership in the Terrorist Financing Targeting Centre (“TFTC”).

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

The UAE is a member of three main regional bodies that issue sanctions – the Arab League, the TFTC and the Gulf Cooperation Council (“GCC”):

- a. Arab League:
The UAE implements sanctions adopted by the Arab League on an *ad hoc* basis.
- b. TFTC:
Members of the TFTC consist of the United States and certain GCC countries.
The UAE implements all sanctions designated by the TFTC by issuing the Local Lists referred to above. TFTC-designated sanctions are also available on the US’s treasury government website.
- c. GCC:
The UAE is a member of the GCC, which consists of six member states. The Charter of the GCC sets up a framework that would permit the joint establishment of foreign policies and therefore issuance of sanctions. Although the GCC has, in the past, made announcements with respect to its members’ stance on foreign policy, it has not, at the date hereof, issued any sanctions as such.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

The UAE maintains two lists of sanctioned individuals and entities:

- a. *Local Lists*: These lists consist of local terrorism lists issued pursuant to Federal Law No. 7 of 2014 on combating terrorism offences (“**Anti-Terrorism Law**”) and the New Sanctions Regulations. Decisions of listing, removal and re-listing on Local Lists enter into effect when issued by the UAE Cabinet and when published in the Official Gazette. Such decisions are also published in audio-visual and print media of the UAE, in both Arabic and English.
- b. *Sanctions List*: This list consists of the sanctions list issued by the UN Security Council. Additions and/or removal from the sanctions list is effected by the UN

Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

The mechanisms available for an individual or entity to challenge its addition to a sanctions list are set out under the New Sanctions Regulations and New SR Guidance:

- a. *Local Lists:* As per Section 9 of the New SR Guidance, the applicant must file a request to the Office, attaching all documents supporting the grievance, in accordance with the relevant UN Sanctions Committee procedures. The Office shall refer the request to the Supreme Council, which shall communicate the request to the UAE Cabinet for its decision. The Office will then notify the applicant of such decision.
- b. *Sanctions List:* The Office set out in the New SR Guidance the procedures of the submission of applications for removal from the Sanctions List. The procedure for submitting a de-listing request is set out under Section 10 of the New SR Guidance and includes, among others, submitting a request/application to the Office, which will then, with the Supreme Council's coordination and subject to its review, forward such request to the UNSC Sanctions Committee.

2.6 How does the public access those lists?

Both the consolidated Local List and Sanctions List are available via the following links:

- a. With respect to the Local List: <https://www.uaecic.gov.ae/>.
- b. With respect to the Sanctions List: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>.

There is also a direct link to the UN sanctions on the Office official website.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

The UAE used to maintain comprehensive sanctions or embargoes on Qatar and Israel; however, these were recently removed and there are no current comprehensive sanctions or embargoes on countries as such. By implementing the UN's sanctions, the UAE does have targeted sanctions against Central African Republic, Congo, Iraq, Libya, Mali, Somalia, South Sudan and Yemen.

2.8 Does your jurisdiction maintain any other sanctions?

In addition to the above-mentioned sanctions, the UAE, in particular, the Central Bank and regulated FIs in the UAE, also takes into consideration sanctions imposed by the EU and OFAC; however, where implemented, such sanctions would be added to its lists accordingly.

2.9 What is the process for lifting sanctions?

The process for lifting sanctions varies depending on the method of imposition as well as the nature of such sanction.

With respect to the Local Lists, the Supreme Council for National Security periodically reviews the same and de-listing applications in coordination with the Ministry of Justice and submits recommendations to the Ministry of Presidential Affairs. The latter then submits the application to the UAE Cabinet, including its opinion. Upon approval, the UAE Cabinet grants the de-listing and publishes it in the Official Gazette.

With respect to sanctions issued by IGOs, sanctions are added and removed by the relevant IGO. The removal of such sanctions is then implemented by the UAE through different means, which may vary depending on the method by which the relevant sanction was imposed.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Although the export control regime of the UAE is distinct from sanctions, it plays an important role in enforcing sanctions where the same is with respect to the export or import of sanctioned products from sanctioned countries/persons. This is particularly illustrated by the significant role accorded to the Office with respect to implementing the Sanctions List, as well as the Commodities Law, which includes banning the import, export or re-export of goods deemed a threat to the UAE's foreign policy (sanctions are often used as an instrument of foreign policy).

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

The UAE does not have blocking statutes or other restrictions prohibiting adherence to other jurisdictions' sanctions or embargoes.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

The UAE does not impose any prohibitions or threaten any sanctions for transactions that do not have a connection to it.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

The parties and transactions subject to UAE's sanctions laws and regulations depend on the nature of and reasons for the sanctions.

Certain sanctions are more narrowly targeted than others. With respect to sanctions targeted at specific individuals and organisations (e.g. under Local Lists), restrictions would not apply based on nationality but rather on identity or affiliations. With respect to more comprehensive sanctions targeted at governments, such sanctions can apply based on the nationality of persons involved.

Sanctions can also apply on the location where the transaction takes place; this is particularly relevant where sanctions are

targeting trade with a certain country or the country imposing the sanction refuses to recognise or accept deals involving the currency of a certain country, as is the case with Iran.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Under Article 15 of the New Sanctions Regulations and under the New SR Guidance, there is an express obligation on FIs, DNFBNs, and all natural and legal persons to block or freeze funds or other property belonging to persons on the sanctions list (“**Designated Persons**”):

- If a match is identified with a Designated Person, they must freeze all funds owned by such person, prohibit the making of funds available, and notify the Office of such measures within two business days of taking such measures.
- In addition to the above, FIs and DNFBNs must set and implement internal controls and procedures as well as policies and procedures to ensure their and their staff’s compliance with the New Sanctions Regulations and that no one tips off any Designated Person of impending measures.

Moreover, Article 5 of the AMLCFT Law specifically accords the governor of the Central Bank or his delegate the right to freeze suspicious funds. Furthermore, Article 2 of the Commodities Law accords the customs departments the right to ban or restrict the import/export of commodities in case the “foreign policy of the [UAE] so requires”.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

There are no licences available that would authorise activities otherwise prohibited by sanctions *per se*. However, special licences may be required to conduct activities more susceptible to the possible breach of sanctions; for example, pursuant to the Commodities Law, strategic goods and dual-use items, such as arms and military hardware, chemical and biological materials, cannot be exported or re-exported without a special licence.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Multiple laws and regulations, including Article 15 of the AMLCFT Law, impose an obligation on FIs and DNFBNs to report to the relevant financial regulator any suspicion or any situation in which they have reasonable grounds to suspect a transaction or funds is related to a money-laundering crime, related predicate offences, financing of terrorism or illegal organisations.

Furthermore, Article 21 of the New Sanctions Regulations and Sections 4(4) and 5 of the Sanctions Implementation Regulations impose several reporting obligations on FIs and DNFBNs to the relevant financial regulator, including in the following cases:

- a. where it has frozen funds pursuant to issued sanctions;
- b. where any of its former customers or an accidental customer dealt with is a person listed on the Sanctions List;
- c. where it has decided not to undertake procedures because of the similarity of names which is unable to be resolved using available or accessible information; and
- d. where it has unfrozen funds/property pursuant to an unfreezing order.

Also, under Section 5 of the New SR Regulations, all UAE natural and legal persons must inform the “*competent authorities*” where they have frozen funds in its possession, under its control, or management, belonging to a Designated Person or to a person representing a Designated Person.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

The government conveys its compliance expectations by circulating circulars and directives as well as issuing laws, regulations and guidance, in particular its New SR Guidance.

Article 16 of the AMLCFT Law, as well as the New SR Guidance, require FIs and DNFBNs to develop internal policies, controls, and procedures to enable them to manage the risks identified and mitigate them. In financial free zones, compliance expectations are comprehensive and included in “*Rulebooks*”. Furthermore, Article 22 of the New Sanctions Regulations imposes an obligation on financial regulators to take all measures to ensure FIs and DNFBNs comply with sanctions and apply administrative sanctions upon violation of such compliance.

A common compliance policy required is the implementation of client due diligence and onboarding clearances to ensure that customers of such institutions are not subject to any sanctions.

At a more general level, Section 5 of the New SR Guidance requires all natural and legal persons to: (1) without delay or prior notice, freeze funds in its possession, under its control or management, belonging to a Designated Person, controlled over, fully or partially, directly or indirectly, or belonging to a person functioning on behalf of a Designated Person, or under its direction, or owned or controlled over by that Designated Person (directly or indirectly); and (2) inform the “*competent authorities*” where they have frozen funds in its possession, under its control, or management, belonging to a Designated Person or to a person representing a Designated Person.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

There are criminal penalties for violating economic sanction laws and/or regulations where such violation also constitutes a crime under Federal Law No. 3 of 1987 on the issuance of the Penal Code (“**Penal Code**”) or other applicable laws, such as the Anti-Terrorism Law, Commodities Law, and AMLCFT Law. Article 23 of the New Sanctions Regulations provides that any violation thereof is subject to the penal and administrative sanctions set forth under the AMLCFT Law. For example, pursuant to Article 28 of the AMLCFT Law, “[i]mprisonment or a fine of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) shall be applied to any person who violates the instruction issued by the competent authority in the UAE for the implementation of the directives of UN Security Council under Chapter (7) of UN Convention for the Suppression of the Financing of Terrorism and Proliferation of Weapons of Mass Destruction and other related decisions”.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The government authorities responsible for investigating criminal economic sanctions offences differ depending on the nature of

the sanctions. As explained above, different government authorities are responsible for implementing different types of sanctions; these very same government authorities must investigate any potential breach by a person under its surveillance. For example, the Central Bank is responsible for investigating any breach of sanctions by FIs, or the relevant customs department for any breach of sanctions by way of unauthorised exports/imports.

These governmental authorities must then report to the executive board of the Supreme Council for National Security or the Public Prosecution as applicable, which will further investigate the matter and may file a claim for prosecution of any person found to be in breach of sanctions through the judiciary system.

4.3 Is there both corporate and personal criminal liability?

There is both corporate and personal criminal liability. This is expressly stated, among others, under Article 42(3) of the Anti-Terrorism Law and Article 4 of the AMLCFT Law.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

Pursuant to Article 42 of the Anti-Terrorism Law, a maximum of AED 100 million shall be imposed upon a judicial person who violates criminal sanctions, unless a more severe penalty is imposed under the Penal Code. Article 162 of the Penal Code provides for a fine of not less than AED 1 million where a person imports/exports to an enemy country in time of war.

Under the Commodities Law, an individual can be fined up to AED 500,000.

4.5 Are there other potential consequences from a criminal law perspective?

Other potential consequences for breach of sanctions, where such breach constitutes crimes under the Anti-Terrorism Law or Penal Code, include imprisonment and capital punishment. The Commodities Law also provides for imprisonment for up to one year. Public prosecution may be involved if the issue relates to a crime punishable by law, such as felonies.

The AMLCFT Law lists potential consequences for breaches thereof, including:

- banning the violator from working in the sector related to the violation for the period determined by the supervisory authority;
- constraining the powers of the board members, supervisory or executive management members, managers or owners who are proven to be responsible for the violation;
- arresting managers, board members and supervisory and executive management members who are proven to be responsible for the violation for a period to be determined by the supervisory authority or requesting their removal; and
- cancelling the licence of the violator.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

There are civil penalties for violating economics sanctions laws and regulations. These penalties depend on the nature of the violation in question.

Persons violating custom laws may find themselves fined or their assets seized and/or destroyed. Persons effecting wire transfers in breach of sanctions may, in certain cases, find access to their bank accounts blocked until an investigation is conducted by the Central Bank or other competent financial regulator.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

The government authority responsible for investigating and enforcing civil economic sanctions would normally be the supervisory authority of the entity/person involved in such breach, but also depends on the nature of the sanction that was breached. For instance: (1) with respect to breach of custom laws, the relevant customs department is responsible; and (2) with respect to breach of the Central Bank's rules, the Central Bank is responsible.

4.8 Is there both corporate and personal civil liability?

There is both corporate and personal liability for civil economic sanctions violations. The laws and procedures applicable where civil economic sanctions are violated include the blocking of transactions and imposition of administrative fines by the competent authorities.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

Administrative penalties may apply where persons are found to have violated economic sanctions; the penalty amount differs depending on the severity of the violation. With respect to customs offences, persons may be fined varying amounts depending on the offence and the value of the related goods. For instance, under Article 28 of the AMLCFT Law, the maximum penalty for violating the sanctions under the Sanctions List is AED 5 million, whereas an FI can be fined up to AED 10 million for the same offence.

4.10 Are there other potential consequences from a civil law perspective?

There is no limitation in principle to other potential consequences for a violation of civil economic sanctions. Other potential consequences may vary depending on the nature of the violation and required measures to avoid a breach of sanctions, including the seizing and destruction of assets and freezing of bank accounts. Notably, pursuant to Article 22 of the New Sanctions Regulations, the supervisory authorities (e.g. Central Bank, DIFC, and so on) have been provided wide jurisdiction to "conducting supervision, control, and follow-up to ensure compliance with the provisions stipulated in [the New Sanctions Regulations] through office and field inspections, and imposing appropriate administrative penalties upon violating its provision or failing to implement them".

Certain companies involved in money laundering and proliferation of dual-use/dangerous materials have had their trade licences revoked due to breach of the AMLCFT Law, sanctions regulations, Commodities Law as well as the Non-Proliferation Treaty and other UN resolutions.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

Assessment of penalties depends on the breach itself. Where the latter includes a transaction, the penalty can be linked to the value of the transaction. Should a matter be brought before the courts, the penalty assessment can also be left to the discretion of the judge. Not all resolutions by the competent authorities are public; certain penalties are imposed at their discretion and are based on the gravity of the violation.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

The appeal process for sanction penalties does not usually take place in judicial proceedings but rather consists of the submission of grievances and other administrative proceedings. Depending on such proceedings, it may be possible in certain cases to raise a claim and to appeal a decision before the courts. The UAE does not have a binding precedent system, therefore information regarding cases in the UAE is not always publicly available.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal and civil enforcement are at both the local and federal level. While the Central Bank administers its applicable laws at a federal level, customs laws are often administered at a local level; for example, with respect to Dubai by the Dubai Customs Department and with respect to Abu Dhabi by the Abu Dhabi Customs Department.

4.14 What is the statute of limitations for economic sanctions violations?

Under Federal Law No. 5 of 1985 regarding civil transactions (“**Civil Code**”), the statute of limitation for civil claims is 15 years, unless otherwise expressly provided in a statute. With respect to money laundering or financing terrorism or crimes by illegal organisations, Article 29(3) of the AMLCFT Law provides that “[t]he criminal case shall not be subject to the statute of limitations for money laundering or financing terrorism or illegal organizations crimes”.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

Additional economic sanctions-related measures are regularly proposed and under consideration; however, such information is not usually shared with the public until officially issued or announced. In other exceptional situations, the UAE may announce its intention to impose or comply with certain sanctions, such as its announcement to comply with existing and upcoming US sanctions on Iran.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

Many economic sanctions laws are available on the websites of the governmental entities issuing the same, sometimes both in English and Arabic. Economic sanctions laws and regulations can also be found in the Official Gazette of the UAE. Guidance, applicable sanctions laws and the Local List and Sanctions List are normally available on the official website of the Office.



Rima Mrad is a Partner with the Corporate and M&A Practice in our DIFC offices in Dubai. She is an experienced corporate and insurance lawyer who has practised in the UAE for over 16 years.

She specialises in advising insurance companies, corporate organisations, financial institutions, energy companies and private equity funds on a wide range of legal issues. These include M&A transactions, due diligence, commercial agreements, commercial related disputes, IT related transactions and various regulatory matters.

She has also advised and assisted international clients in developing their business throughout the GCC, particularly in relation to regulatory and compliance matters. She also provides employment advice to companies in relation to policies, structuring and breach of contract.

Rima was recently recognised by *Financial News* as the 50 Most Influential Women in the Middle East Finance – 2019.

Rima holds a Master's Degree in Public Law and Sustainable Development Law from Université Paris Descartes.

BSA Ahmad Bin Hezeem & Associates LLP DIFC

Building 3, East Wing, Level 6
Dubai International Financial Centre
Dubai
United Arab Emirates

Tel: +971 4 528 5555
Email: rima.mrad@bsabh.com
URL: www.bsabh.com



Tala Azar is an Associate in the Corporate and M&A Practice in our DIFC office in Dubai. She has over four years' legal experience in cross-border and domestic mergers and acquisitions, other commercial and financial transactions, joint ventures, corporate restructuring and general corporate matters. Tala regularly represents private clients on general transactional and contractual work.

Tala holds an LL.B. in French law from Université Paris X (Nanterre) and an LL.B. in English Law with Honours from the University of Kent.

Tala is also admitted to practise in the State of New York and is fluent in English, French and Arabic.

BSA Ahmad Bin Hezeem & Associates LLP

Building 3, East Wing, Level 6
Dubai International Financial Centre
Dubai
United Arab Emirates

Tel: +971 4 528 5555
Email: tala.azar@bsabh.com
URL: www.bsabh.com

We are a team of legal experts who fully understand all aspects of doing business in the Middle East. Our vision is to create a 'trusted-adviser' service of real, tangible value to you. We are therefore excited about the prospect of working with you and building a long-lasting relationship between us.

Many law firms can give you legal advice in the Middle East. However, very few have started out in Dubai and grown to encompass the UAE, Saudi Arabia, Oman, Lebanon, and Iraq. So, what makes us different? Well, let's just say: it's not what we do but the way that we do it.

Of course, as a full-service law firm, we have a comprehensive knowledge of local laws and customs. Our people are fluent in a range of languages including Arabic, English and French. And we have access to the relevant local authorities and rights of audience before all the courts.

Our areas of focus include: Arbitration and Dispute Resolution, Banking and Finance, Commercial, Construction, Corporate and M&A, Employment, Energy and Engineering, Insurance and Reinsurance, Intellectual Property, Litigation, Real Estate, Tax and VAT and Technology, Media, and Telecom. But it's the way we interact with our clients that sets us apart from the crowd. Our modernised and progressive approach means we'll talk to you

in a straightforward manner and bring innovation to everything we do, from management information to case handling and billing.

We help people do business all over the world. It doesn't matter what sector or jurisdiction you operate in or whether you're a fledgling regional business or a multi-national corporate. With five offices in the Middle East, another in France and affiliates across Asia, Europe and the US, we can help you negotiate the maze of global regulations and ensure your interests are protected at all times.

www.bsabh.com

BSA
BSA Ahmad Bin Hezeem
& Associates LLP

United Kingdom

HFW



Daniel Martin

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

The UK sanctions regime broadly falls into two categories, namely: sanctions adopted to implement UN sanctions, in compliance with the UK's obligations; and together with additional, national measures which go beyond the UN sanctions.

The regime and legal basis for the UK's national measures changed following the UK's departure from the European Union (EU). Since 1 January 2021, the UK has adopted purely national measures (although, to date, there have only been limited differences between the UK and the EU position).

The over-arching legislation is the Sanctions and Anti-Money Laundering Act 2018 and individual targeted sanctions programmes are promulgated by secondary legislation pursuant to the Sanctions and Anti-Money Laundering Act 2018. Those include country-specific sanctions (for example, sanctions against Iran) or sanctions targeting issues which are not specific to a particular country (such as sanctions targeting terrorist activities, as well as sanctions targeting serious human rights violations and abuses around the world).

The Act identifies six main types of sanctions, as follows: (i) financial sanctions; (ii) immigration sanctions; (iii) trade sanctions; (iv) aircraft sanctions; (v) shipping sanctions; and (vi) "other sanctions for purposes of UN obligations".

The financial sanctions include prohibitions on the provision of financial services and asset freezes which, amongst other things, prohibit dealing in the property of designated persons and make it an offence for other persons to make funds or economic resources available to or for the benefit of designated persons.

The trade sanctions include measures which, amongst other things, prohibit the export of certain goods, prohibit the import of certain goods, prevent the transfer of certain technology and prevent the provision of certain services.

The aircraft sanctions include restrictions on disqualified aircraft and also contain restrictions on owning, chartering, operating or registering certain aircraft.

The shipping sanctions include restrictions on disqualified ships and also contain restrictions on owning, chartering, operating or registering certain ships.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

The Office of Financial Sanctions Implementation (OFSI), which is a part of HM Treasury, is responsible for ensuring that

financial sanctions are properly understood, implemented and enforced in the United Kingdom.

The Export Control Joint Unit (ECJU), which is part of the Department for International Trade (DIT), administers the UK's system of export controls and licensing for military and dual-use items.

A number of other UK Government departments and agencies also have a role, including the Foreign & Commonwealth Office (FCO), Department for Transport (DfT) and the National Crime Agency (NCA).

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

In November 2020, Giles Thomson took over as OFSI Director and reiterated OFSI's commitment to "*robustly but fairly and proportionately use the compliance tools available to us, including monetary penalties, to effectively enforce financial sanctions in the UK*". In March 2021, clarificatory changes were made to UK guidance on monetary penalties.

There have been developments with respect to sanctions against Belarus, as well as the sanctions targeting global corruption.

In January 2021, the UK published the first general licence – this enables payments to Crimean sea ports to be made out of non-frozen funds and obviates the need for a specific licence.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Sanctions are imposed under the authority of the Sanctions and Anti-Money Laundering Act 2018.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

The UK implements UN sanctions. These are implemented via secondary legislation (statutory instruments) pursuant to the Sanctions and Anti-Money Laundering Act 2018.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

Following the UK's departure from the EU, the UK currently adopts purely national measures.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

Yes. Persons will either be designated pursuant to powers contained in the relevant regulation that authorise an appropriate Minister to designate persons for the purposes of those regulations or because those persons are named by or under UN Security Council Resolutions. Likewise, a designation may be varied or revoked by the Minister.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Yes. The designated person may request the Minister either to vary or revoke the designation.

2.6 How does the public access those lists?

OFSI maintains a consolidated list of asset freeze targets and this is available on its website at <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

No: UK sanctions are targeted, rather than comprehensive. The full extent of the restrictions varies from regime to regime, but the restrictions fall short of full embargoes.

2.8 Does your jurisdiction maintain any other sanctions?

The UK adopts both country-specific sanctions (for example, sanctions against Iran) and also sanctions which target issues which are not specific to a particular country.

The non-country-specific sanctions include sanctions relating to chemical weapons, cyber-attacks, terrorism and terrorist financing, and serious human rights violations and abuses around the world.

2.9 What is the process for lifting sanctions?

The Sanctions and Anti-Money Laundering Act 2018 contains a mechanism for the periodic review of sanctions programmes – that covers not only a review of the designations under the relevant programme, but also a review of whether the regulations themselves are still appropriate.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

Yes – the UK has an export control regime under the Export Control Act 2002 and the Export Control Order 2008.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

Yes, pursuant to the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) Order 1996 and the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) (Amendment) Order 2018.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

The UK does not currently impose secondary sanctions.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction's sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

UK sanctions pursuant to the Sanctions and Anti-Money Laundering Act 2018 impose prohibitions or requirements in relation to either (a) conduct in the United Kingdom or in the territorial sea by any person, or (b) conduct elsewhere, but only if the conduct is by a United Kingdom person. A United Kingdom person means a United Kingdom national or a body incorporated or constituted under the law of any part of the United Kingdom.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

Yes. A person (P) must not deal with funds or economic resources owned, held or controlled, by a designated person if P knows, or has reasonable cause to suspect, that P is dealing with such funds or economic resources. A firm which holds funds of a designated person must freeze those funds and report to OFSI.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes – particular regulations may contain provisions which allow licences to be granted, for example, to enable the basic needs of a designated person to be met. A licence may only be granted in the circumstances set out in the relevant regulation, and may be subject to conditions and reporting requirements.

Applications should be made as early as possible and at least four weeks before a licence is needed. OFSI prioritises humanitarian applications and will process urgent applications where there are life-threatening circumstances.

Applicants should provide as full an explanation as possible of the proposed transaction for which they need a licence. In order to licence a transaction which would otherwise be prohibited by financial sanctions, OFSI will require information on (a) the amount of the intended payment, (b) the intended purpose of the transaction/funds, (c) the intended payment route, (d) the sender and receiver of funds, including any intermediaries and beneficiaries, and (e) how the funds will be accounted for.

Licence applications must be submitted via the financial sanctions licence application form which can be found at https://www.gov.uk/government/uploads/system/uploads/attachment_t_data/file/448158/Generic_Licence_Application_Form.doc.

These licences should not be confused with export control licences issued by the ECJU, which permit prohibited activity under trade sanctions or export controls.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Yes, there are reporting obligations on financial institutions and others (including law firms) to report as soon as practicable if it knows, or has reasonable cause to suspect, that a person is a designated person or has committed certain offences under the regulations.

The report must contain the information or other matter on which the knowledge or suspicion is based, and any information which the reporting party holds about the other person and information about any funds or economic resources which are held. OFSI provides a frozen asset reporting template to facilitate this process.

OFSI also conducts an annual frozen funds reporting exercise, whereby persons holding frozen funds must provide up to date details as of a specified date (usually in the Autumn) to OFSI.

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

OFSI offers an email alert service and has published guidance on a number of topics, including general guidance and guidance for particular sectors (currently there is guidance for each of the charity, import/export and maritime sectors), as well as a blog which covers topics such as “Am I dealing with a sanctioned entity?”.

OFSI does not mandate a particular compliance programme, or the use of particular tools or products. OFSI expects businesses to be aware of and comply with the law, and has indicated that, whilst each person and each business should make their own assessment of what is reasonable and necessary for their particular circumstances, OFSI will take account of the level of actual or expected knowledge and the extent of relevant ways of complying when dealing with any breach.

OFSI recognises that some searches are straightforward and others are more difficult (for example, where companies have more complicated ownership structures and checks beyond the scope of OFSI’s consolidated list are required to establish who owns them).

Specific requirements may be imposed by sector regulators, for example, the Financial Conduct Authority (FCA) requires that regulated bodies have adequate systems and controls in

place to mitigate financial crime risk, including in respect of sanctions. The FCA provides specific guidance in Chapter 7 of Part 1 of the handbook *Financial Crime: A Guide for Firms*.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes. The regulations set out the relevant penalties, but these can include unlimited fines and up to seven years’ imprisonment.

Deferred Prosecution Agreements (DPAs) were introduced in the UK in February 2014, under the provisions of Schedule 17 of the Crime and Courts Act 2013, and these are available in cases where a prosecutor has charged a company with a breach of sanctions. Under a DPA, a prosecutor charges a company with a criminal offence but proceedings are automatically suspended if the DPA is approved by the judge.

OFSI also has powers, pursuant to the Policing and Crime Act 2017, to impose monetary penalties for breaches of financial sanctions, such as a breach of the asset freeze.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

Whilst OFSI is responsible for ensuring that financial sanctions are properly understood, implemented and enforced, cases will be handed over to the Crown Prosecution Service (CPS), which decides whether cases should be prosecuted, based on the quality of the evidence and whether a prosecution is needed in the public interest.

The NCA is the law enforcement agency responsible for the investigation of the most serious cases of sanctions evasion.

4.3 Is there both corporate and personal criminal liability?

Yes. Fines can be imposed on both individuals and companies.

Where an offence under the applicable regulations has been committed by a body corporate either with the consent or connivance of any director (or equivalent), or where the offence is attributable to any neglect on the part of any such person, that person, as well as the body corporate, is guilty of the offence and is liable to be proceeded against and punished accordingly.

The Crown Prosecution Service has published guidance which sets out the common approach of the Director of Public Prosecutions and the Director of the Serious Fraud Office to the prosecution in England and Wales of corporate offending and makes clear their view that a thorough enforcement of the criminal law against corporate offenders, where appropriate, will have a deterrent effect, protect the public and support ethical business practices.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

The relevant regulation will set out the maximum fine, which may be unlimited.

4.5 Are there other potential consequences from a criminal law perspective?

There is also scope for imprisonment of individuals.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

The monetary penalties regime created by the Policing and Crime Act 2017 provides an alternative to criminal prosecution for breaches of financial sanctions legislation.

OFSI may impose a monetary penalty on a person if it is satisfied, on the balance of probabilities, that (a) the person has breached a prohibition, or failed to comply with an obligation, that is imposed by or under financial sanctions legislation, and (b) the person knew, or had reasonable cause to suspect, that the person was in breach of the prohibition or (as the case may be) had failed to comply with the obligation.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

OFSI imposes these monetary penalties.

4.8 Is there both corporate and personal civil liability?

A monetary penalty may be imposed on a “person”, which means a body of any type, or an individual.

If a monetary penalty is payable by a corporate, OFSI may also impose a monetary penalty on an officer of the body where the breach (a) took place with the consent or connivance of the officer, or (b) was attributable to any neglect on the part of the officer.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

Where the breach or failure relates to particular funds or economic resources and it is possible to estimate the value of the funds or economic resources, the permitted maximum is the greater of (a) £1,000,000, and (b) 50% of the estimated value of the funds or resources. In any other case, the permitted maximum is £1,000,000.

4.10 Are there other potential consequences from a civil law perspective?

The Policing and Crime Act 2017 extended the availability of Serious Crime Prevention Orders (SCPOs) pursuant to the Serious Crime Act 2007 so that they could be imposed in cases of breaches of sanctions.

An SCPO is a court order that is used to protect the public by preventing, restricting or disrupting a person’s involvement in serious crime. It achieves this by imposing targeted prohibitions, restrictions and/or requirements on a person who has been involved in serious crime, in order to prevent further breaches. In the case of sanctions breaches, an SCPO could be used to require the adoption of a sanctions compliance procedure.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

OFSI can respond to a breach of financial sanctions in several ways, depending on the case. This could range from issuing correspondence requiring details of how a party proposes to improve their compliance practices to imposing a monetary penalty or referring the case to law enforcement agencies for criminal investigation and potential prosecution.

OFSI takes a number of factors into account, including whether there has been direct provision of funds or economic resources to a designated person, whether there has been circumvention of sanctions, the value of the breach, the harm to the sanctions regime’s objectives, and the behaviour of the relevant party (including any voluntary disclosure which has been made).

OFSI calculates the penalty via a three-stage process. The first stage is determining whether the penalty threshold has been met (i.e. there has been a breach and a monetary penalty is appropriate and proportionate). The second stage is calculation of the baseline penalty, starting from the statutory maximum penalty and then assessing what level of penalty is reasonable and proportionate, applying a discount of up to 50% where there has been a prompt and complete voluntary disclosure of a breach. The third stage is a penalty recommendation (as the person on whom OFSI intends to impose a penalty then has a right to make representations).

OFSI will normally publish details of all monetary penalties it imposes, but will normally only publish a summary of the case. If OFSI determines that it is not appropriate or not in the public interest to publish a summary, they may publish an anonymised report.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Once a monetary penalty has been imposed, the person on whom OFSI has imposed the penalty has a right to seek a ministerial review of the decision. The person will normally have 28 calendar days to inform OFSI that they want a review. That review is normally carried out by the Economic Secretary to the Treasury (EST).

If a person has sought ministerial review, and a penalty is still imposed, they can then appeal to the Upper Tribunal. A notice of appeal must be made in writing and received by the Upper Tribunal no later than 28 days after notice was given of the decision under challenge.

In April 2020, OFSI announced that it had imposed a penalty of £20.47 million on Standard Chartered Bank for breaches of EU sanctions, specifically for making loans to a subsidiary of a Russian bank in breach of a prohibition on making loans or credit, or being part of an arrangement to make loans or credit, available to sanctioned entities, where those loans or credit have a maturity of over 30 days.

Because Standard Chartered Bank disclosed the suspected breaches of financial sanctions to OFSI, carried out an internal investigation of the breaches, provided a detailed report of the investigation to OFSI, as well as interim updates, and cooperated with OFSI’s investigation, OFSI reduced each penalty by 30% (from £45 million to £31.5 million).

Standard Chartered exercised its right to a Ministerial review. The Minister upheld OFSI’s decision to impose the penalty, but materially reduced the overall penalty (from a total of £31.5 million to a total of £20.47 million). He did so on the basis that,

while the mitigating factors mentioned above had been considered in OFSI's assessment, they should have been given more weight in the penalty recommendation.

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Criminal and civil enforcement is only at the national level.

4.14 What is the statute of limitations for economic sanctions violations?

The UK does not have a statute of limitations for criminal offences, so there is no time limit for criminal proceedings for a breach of sanctions.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

We expect that the UK will continue its use of thematic sanctions as well as country-wide sanctions, in order to pursue broad policy objectives. While the UK is likely to adopt further autonomous measures, we anticipate that there will only be limited divergence from EU sanctions over the next 12 months.

It is likely that there will be future enforcement with penalties imposed for breaches of UK sanctions, but there will also be continued engagement between OFSI and industry and other interested parties.

Finally, we expect continued difficulty and tension over sanctions with respect to Iran and Russia, with those sanctions measures likely to remain in place over the next 12 months.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

- The Sanctions and Anti-Money Laundering Act 2018 can be accessed at https://www.legislation.gov.uk/ukpga/2018/13/pdfs/ukpga_20180013_en.pdf.
- OFSI's website contains information about the various sanctions regimes. These can be accessed at <https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>.
- The list of all asset freeze targets can be accessed (in a variety of formats) at <https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets>.
- OFSI's guidance, FAQs and information on monetary penalties can be accessed at <https://www.gov.uk/government/publications/financial-sanctions-faqs>.
- OFSI publishes information about actions by OFSI to enforce financial sanctions at <https://www.gov.uk/government/collections/enforcement-of-financial-sanctions>.
- OFSI publishes free email alerts and the page to sign up for these is <https://public.govdelivery.com/accounts/UKHMTREAS/subscriber/new>.

All material is available in English.



Daniel Martin advises traders, shipowners, freight forwarders, insurers and brokers on a host of regulatory and compliance issues, including international trade sanctions, export controls, customs and anti-corruption legislation. He advises on all aspects of the EU and UK sanctions legislation, and he is also familiar with the application of US sanctions to non-US persons.

As well as advice on dispute resolution, customs and regulatory compliance (including ways to engage effectively with HMRC and other regulators), Daniel also advises on compliance procedures and controls which traders, shipowners, logistics companies, banks, insurers and brokers should adopt to minimise risk.

Acritas Star Lawyers describes Daniel as “down to earth, commercially minded, understands my business and thinking outside the box”.

HFW

Friary Court, 65 Crutched Friars
London EC3N 2AE
United Kingdom

Tel: +44 20 7264 8189
Email: daniel.martin@hfw.com
URL: www.hfw.com

HFW is a sector-focused global law firm.

We have over 600 lawyers working across the Americas, Europe, the Middle East, Asia and Australia. We take a progressive approach to our roles in commercial business – thinking creatively and pragmatically to support our clients.

Whether we are solving complex issues within the construction, aviation or shipping industries, or providing advice across insurance, commodities and energy, we are specialist lawyers here to add value to our clients. We think about the commercial solution first, and then underpin our advice with a solid foundation of legal expertise.

www.hfw.com

USA

Paul, Weiss, Rifkind, Wharton & Garrison LLP



Roberto J. Gonzalez



Rachel M. Fiorill

USA

1 Overview

1.1 Describe your jurisdiction's sanctions regime.

The U.S. Government maintains a range of economic sanctions, administered primarily by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"). Most U.S. sanctions are considered "primary sanctions". To violate U.S. primary sanctions, a transaction must generally involve both (i) a U.S. nexus, and (ii) a sanctioned person (entities or individuals) or a sanctioned jurisdiction. A transaction can have a U.S. nexus if it involves a U.S. person or U.S.-origin products, software, or technology, or if it causes or involves activity within U.S. territory. Importantly, non-U.S. companies and individuals can engage in U.S.-nexus transactions and thereby violate U.S. sanctions.

Primary sanctions encompass several types of sanctions:

- **List-based blocking sanctions** generally prohibit U.S.-nexus transactions with designated persons (individuals, entities, vessels, aircraft, etc.), which OFAC has placed on its Specially Designated Nationals ("SDN") List. OFAC maintains a number of sanctions programmes, including country-specific programmes and programmes targeting international narcotics trafficking, proliferation, malicious cyber activity, and other illicit activity. OFAC has authority to designate persons that satisfy a programme's criteria and to add those persons to the SDN List. Any property or property interests of SDNs that come within U.S. jurisdiction must be "blocked" or frozen. The blocked funds must be placed into separate suspense accounts and cannot be released absent specific authorisation from OFAC. (List-based sanctions are discussed below in question 2.4.)
- **Targeted sanctions** generally prohibit *specified* U.S.-nexus dealings with particular persons. For example, under the Russia/Ukraine sanctions programme, so-called "sectoral sanctions" prohibit certain categories of activity with persons designated on the Sectoral Sanctions Identification ("SSI") List from four sectors of the Russian economy (financial, energy, defence, and oil exploration/production). (These sanctions are discussed further below in question 2.8.) Another example is the new sanctions programme prohibiting U.S. person investment in certain Chinese companies' securities.
- **Comprehensive country or region sanctions** broadly target countries or regions (together, "jurisdictions") and generally prohibit almost all U.S.-nexus transactions with those jurisdictions. Currently, there are five jurisdictions subject to comprehensive U.S. sanctions:

Cuba; the Crimea region; Iran; North Korea; and Syria. In addition, pursuant to "secondary sanctions", the U.S. government has threatened to sanction non-U.S. persons that engage in specific activities involving targeted countries, industries, and/or persons, even in the absence of a U.S. nexus. Secondary sanctions are discussed further below at question 2.12.

These various forms of U.S. sanctions can co-exist. For example, with respect to Russia, there is a U.S. embargo on the Crimea region, various Russian companies and individuals have been designated SDNs or SSIs, and specified activities in Russia are subject to the threat of secondary sanctions.

1.2 What are the relevant government agencies that administer or enforce the sanctions regime?

OFAC administers and enforces economic sanctions based on U.S. foreign policy and national security goals.

Jurisdictions become the target of U.S. sanctions by means of executive orders signed by the President of the United States ("the President"). Persons can become the target of U.S. sanctions by being named in executive orders or by OFAC's exercise of authority delegated by the President (where the President provides criteria for imposing sanctions), in consultation with the U.S. State Department and sometimes other agencies (such as the U.S. Department of Justice ("DOJ")). OFAC also has primary responsibility for licensing transactions that would otherwise be prohibited by U.S. sanctions. Additionally, OFAC has the power to investigate and impose civil monetary penalties against persons (including non-U.S. persons) that violate U.S. sanctions laws and regulations.

The DOJ criminally investigates and prosecutes "wilful" violations of U.S. sanctions. The federal banking agencies, including the Office of the Comptroller of the Currency and the Federal Reserve Board of Governors, also have the authority to impose civil penalties for violations of U.S. sanctions laws and regulations. The New York Department of Financial Services (which supervises certain financial institutions operating in New York) also plays a high-profile role in sanctions enforcement under New York state-law requirements.

Finally, the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") administers and enforces U.S. anti-money laundering laws. Its Section 311 authority under the USA PATRIOT Act to designate a jurisdiction or non-U.S. entity as of "primary money laundering concern" can have effects similar to sanctions.

1.3 Have there been any significant changes or developments impacting your jurisdiction's sanctions regime over the past 12 months?

There have been a number of developments and updates to U.S. sanctions over the course of the last year. The most notable recent trend in these changes has been the U.S. government's continued focus on China. There have been several SDN designations of Chinese companies and Chinese government officials during the last year, largely relating to the Xinjiang Uyghur Autonomous Region ("XUAR") and Hong Kong. OFAC also issued an updated supply chain advisory alerting companies to sanctions-related risks of doing certain types of business in or sourcing items from the XUAR. Additionally, in June 2021, President Biden revamped what had been introduced in late 2020 as the "Communist Chinese Military Companies" ("CCMC") sanctions programme. The revamped sanctions programme, now the "Chinese Military Company ("CMC") Sanctions", largely retains the same prohibitions as the CCMC sanctions (*i.e.*, the CMC sanctions prohibit U.S. persons from purchasing or selling any publicly traded securities entities included on the Chinese Military-Industrial Complex ("CMIC") List), but expands the criteria for designation as a CMIC beyond association with the Chinese military to also reflect specific concern for Chinese surveillance technology.

Beyond China, OFAC has continued to make a number of other sanctions designations over the course of the last year, the most notable of which related to Burma (Myanmar), Cuba, Russia, and human rights abuses under the Global Magnitsky sanctions programme.

2 Legal Basis/Sanctions Authorities

2.1 What are the legal or administrative authorities for imposing sanctions?

Under various statutory authorities, the President has broad discretion to regulate commerce where there is an unusual and extraordinary threat from outside the United States to the United States' national security, foreign policy or economy. The President imposes new sanctions programmes and exercises his sanctions-related powers by means of executive orders and then delegates administration of specific sanctions programmes to U.S. agencies, with much of this administration being delegated to the U.S. Treasury Department. Executive orders sometimes have an annex in which the President himself sanctions certain persons, in addition to providing criteria for further designations. Executive orders can also prohibit certain activities, such as imports or exports to certain countries or regions. In some instances, Congress will enact or codify certain sanctions, which then limits the President's discretion.

The International Emergency Economic Powers Act ("IEEPA"), Title II of Pub. L. 95-223, 91 Stat. 1626, codified at 50 U.S.C. §§ 1701 *et seq.*, is the main source of statutory authority for most U.S. sanctions programmes. Other statutory authorities include the Trading with the Enemy Act, which is the basis of the Cuba sanctions programme, and the Foreign Narcotics Kingpin Designation Act. Congress has also passed a series of laws authorising or requiring sanctions targeting particular jurisdictions or activities. For example, in 2017, Congress passed and the President signed the Countering America's Adversaries Through Sanctions Act ("CAATSA"), which expands sanctions targeting Iran, North Korea and Russia.

2.2 Does your jurisdiction implement United Nations sanctions? Describe that process. Are there any significant ways in which your jurisdiction fails to implement United Nations sanctions?

Generally, yes. Almost all jurisdictions and persons that are the target of United Nations sanctions are also the target of U.S. sanctions. The imposition of U.S. sanctions on U.N.-designated parties follows OFAC's standard process of making such designations under existing sanctions programmes or, in some cases, the President issues an executive order empowering OFAC to make such designations.

2.3 Is your jurisdiction a member of a regional body that issues sanctions? If so: (a) does your jurisdiction implement those sanctions? Describe that process; and (b) are there any significant ways in which your jurisdiction fails to implement these regional sanctions?

The United States is a member of numerous regional bodies. To the extent such bodies call upon members to impose sanctions (which, to date, has been rare), the United States is normally a participant.

2.4 Does your jurisdiction maintain any lists of sanctioned individuals and entities? How are individuals and entities: a) added to those sanctions lists; and b) removed from those sanctions lists?

OFAC maintains a number of lists of sanctioned individuals and entities, the most significant of which is the SDN List. These lists include:

- **SDN List:** U.S. law generally prohibits U.S.-nexus transactions with the thousands of individuals, companies, vessels, and other entities on the SDN List. Also, U.S. persons (including, in the case of Cuba and Iran sanctions, non-U.S. companies owned or controlled by U.S. companies) are required to "block" the property and property interests of SDNs. "Blocking" is discussed further at question 3.2 below. The SDN List is available on OFAC's website (<https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>).
- **Foreign Sanctions Evaders ("FSE") List:** OFAC may designate persons for violating, attempting to violate, conspiring to violate, or causing a violation of U.S. sanctions imposed on Syria or Iran, and such persons are placed on the Foreign Sanctions Evaders List. This list also includes non-U.S. persons determined by OFAC to have facilitated deceptive transactions for or on behalf of sanctioned persons. U.S.-nexus transactions with persons on the FSE list are generally prohibited, but, unlike the SDN List, there are no blocking requirements.
- **SSI List:** This list contains entities from four sectors of the Russian economy (financial, energy, defence, and oil exploration/production). Certain categories of U.S.-nexus dealings with entities on the SSI List are generally prohibited. The SSI List is discussed further at question 2.8 below.
- **Non-SDN CMIC List:** This list identifies the Chinese companies subject to the CMC sanctions further discussed at question 1.3 above. U.S. persons are generally prohibited from purchasing or selling any publicly traded securities of entities included on the non-SDN CMIC List.
- **Correspondent Account or Payable-Through Account Sanctions ("CAPTA") List:** This list contains non-U.S.

financial institutions for which the opening or maintaining of a correspondent account or a payable-through account in the United States is prohibited or is subject to one or more strict conditions, pursuant to Hizballah, Iran, North Korea and Russia/Ukraine-related sanctions. The specific sanctions applying to each sanctioned entity are enumerated within the CAPTA List.

Notably, under OFAC's "50 per cent rule", any entity that is 50 per cent or more owned directly or indirectly by one or more SDNs is considered blocked (*i.e.*, treated as an SDN) even though it does not appear on the list. The ownership interests of multiple SDNs in a single entity are aggregated for the purposes of this rule. For example, if SDN X owns 25 per cent of Entity A, and SDN Y owns another 25 per cent of Entity A, Entity A is treated as an SDN. The 50 per cent rule also applies to SSI entities.

The U.S. Department of State also maintains sanctions lists, including certain non-proliferation sanctions, which it coordinates with OFAC such that entities designated are also designated on OFAC's sanctions lists.

2.5 Is there a mechanism for an individual or entity to challenge its addition to a sanctions list?

Yes. Individuals or entities that are designated on an OFAC sanctions list may submit a request for removal to OFAC that provides reasons why the circumstances resulting in the designation no longer apply and/or the designation was in error. In the case of the SDN List, such requests for removal are governed by 31 C.F.R. § 501.807. If OFAC declines, this decision may be challenged in court.

2.6 How does the public access those lists?

OFAC maintains copies of its sanctions lists on its website and has a consolidated search function for all of the lists available (<https://sanctionssearch.ofac.treas.gov/>). OFAC also publishes notices of additions or removals to its sanctions list on its website and distributes them by email. This information is also published in the Federal Register.

2.7 Does your jurisdiction maintain any comprehensive sanctions or embargoes against countries or regions?

The United States maintains comprehensive sanctions against Cuba; the Crimea region; Iran; North Korea; and Syria. With limited exceptions, U.S. nexus-transactions with these countries or regions are prohibited.

2.8 Does your jurisdiction maintain any other sanctions?

Yes, under the category of "primary sanctions", OFAC maintains certain "sectoral sanctions" under the Russia/Ukraine sanctions programme. Sectoral sanctions were designed to impose a "targeted" impact on the Russian economy, as compared to more traditional OFAC sanctions. These sanctions prohibit certain categories of dealings involving U.S. persons or U.S. territory with parties named on OFAC's SSI List. OFAC has issued four directives (the "Directives"), with each directive targeting a different sector of the Russian economy: financial; energy; defence; and oil exploration/production. Generally, the Directives prohibit U.S.-nexus transactions that involve certain

enumerated activities with SSIs designated from these four sectors of the Russian economy. For the first three sectors, the prohibited transactions involve certain equity and debt transactions. OFAC applies its 50 per cent rule (discussed above at question 2.4) to SSIs.

The U.S. Government has also imposed a series of sanctions targeted at the Maduro regime in Venezuela, the most significant of which imposed a blocking order on the Government of Venezuela (including entities owned or controlled by the Government of Venezuela), with certain limited exceptions.

2.9 What is the process for lifting sanctions?

Generally, the President has the authority to rescind or amend an executive order to change the nature of, or completely remove, a sanctions programme. However, some sanctions programmes (such as the U.S. embargo against Cuba) are set by statute either in whole or in part, and Congress would have to pass new legislation for such sanctions to be fully lifted.

As for sanctions against specific individuals or entities, OFAC normally has the authority to remove persons from its sanctions lists, subject to interagency consultation.

2.10 Does your jurisdiction have an export control regime that is distinct from sanctions?

The United States has two main export control regimes: (i) the Export Administration Regulations ("EAR") administered by the U.S. Commerce Department's Bureau of Industry and Security ("BIS"); and (ii) the International Traffic in Arms Regulations ("ITAR") administered by the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC"). The EAR controls the export, reexport, and in-country transfer of most U.S. origin items, software, and technology (including items manufactured outside the United States that contain a certain amount of controlled U.S.-origin content). The ITAR controls the export and retransfer of, as well as brokering in, U.S. defence articles and technologies listed on the U.S. Munitions List. Violations of the EAR and ITAR are subject to civil and criminal penalties.

2.11 Does your jurisdiction have blocking statutes or other restrictions that prohibit adherence to other jurisdictions' sanctions or embargoes?

The United States has certain "anti-boycott" laws and regulations, administered by BIS, that prohibit U.S. persons from participating in non-U.S.-sanctioned boycotts (*i.e.*, boycotts of which the U.S. Government does not approve). Currently, the most notable such boycott is the Arab League's boycott of Israel.

2.12 Does your jurisdiction impose any prohibitions or threaten any sanctions consequences for transactions that do not have a connection to that jurisdiction (sometimes referred to as "secondary sanctions")?

The U.S. government utilises "secondary sanctions" to discourage certain specified activities by non-U.S. persons that do not involve a U.S. nexus. These sanctions threaten to place a non-U.S. person on the SDN List (or impose other, lesser sanctions) if the non-U.S. person engages in certain identified activities. For example, under Executive Order 13810, non-U.S. persons that engage in a range of activities involving

North Korea – whether or not those transactions have a U.S. nexus – may be added to the SDN List. In these situations, the U.S. government effectively forces non-U.S. persons to choose between engaging with the United States and engaging in activity with the sanctions target. Importantly, while the consequences of violating primary sanctions is a potential enforcement action, secondary sanctions cannot be “violated” because they are threats, not legal prohibitions. The consequence for engaging in activities that are the subject of these threats is designation on the SDN List or the imposition of some other trade restriction with the United States.

Secondary sanctions can be threatened by the President through an executive order or can be threatened by Congress in legislation that either requires or authorises the President to impose sanctions on parties that engage in certain types of activities. The President maintains significant discretion even with respect to imposing “mandatory” secondary sanctions, because such authorities require the President to sanction persons that the President determines have engaged in certain activities, and the President enjoys discretion as to whether to make such determinations.

Currently, the U.S. government threatens secondary sanctions against non-U.S. persons for specified activities involving Hizballah, Iran, North Korea, Russia, and Venezuela. The U.S. government also threatens certain secondary sanctions against non-U.S. financial institutions that conduct certain “significant” transactions with persons that are the target of certain terrorism-related sanctions. Due to the enactment of the Hong Kong Autonomy Act in July 2020, secondary sanctions are also threatened against non-U.S. financial institutions that participate in certain “significant” transactions with persons identified as having contributed to the undermining of Hong Kong’s autonomy. Non-U.S. companies with activities involving these countries, entities, or individuals should carefully evaluate any applicable secondary sanctions.

3 Implementation of Sanctions Laws and Regulations

3.1 What parties and transactions are subject to your jurisdiction’s sanctions laws and regulations? For example, do sanctions restrictions apply based on the nationality of the parties involved? Or the location where the transactions take place?

To violate U.S. primary sanctions, a transaction must generally involve both (i) a U.S. nexus, and (ii) a sanctioned person or jurisdiction. A U.S. nexus can arise in a variety of ways, including the involvement of U.S. persons (defined below), the involvement of U.S.-origin products, software, or technology, or causing or involving activity within U.S. territory (such as the use of U.S. dollar transactions that transit the U.S. financial system). OFAC generally defines a “U.S. person” to include: any U.S. citizen, wherever located; any U.S. permanent resident alien, wherever located; any entity organised under the laws of the United States or any jurisdiction within the United States (including non-U.S. branches of U.S. banks); or any person while present in the United States. With respect to the Cuba and Iran sanctions programmes, non-U.S. entities owned or controlled by United States persons are also considered to be “U.S. persons”.

Accordingly, any U.S.-nexus transactions with parties listed on the SDN or FSE lists are generally prohibited. It is also generally prohibited to engage in U.S.-nexus transactions that directly or indirectly involve comprehensively sanctioned jurisdictions, including companies organised under the laws of a

sanctioned jurisdiction, the governments of sanctioned jurisdictions, persons usually resident in sanctioned jurisdictions, and third-country entities or individuals (including so-called “front companies”) where the benefits of the transaction will flow to a sanctioned jurisdiction.

Importantly, non-U.S. persons can conduct transactions that have a U.S. nexus. Examples include transactions involving U.S. person employees or U.S. business partners, financial transactions that are processed through the U.S. financial system (including non-U.S. branches of U.S. banks), or the export or reexport of U.S.-origin goods. Further, OFAC’s sanctions programmes generally prohibit transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC. Non-U.S. persons may expose themselves to U.S. sanctions liability by “causing” a violation of primary sanctions by U.S. persons or involving U.S. territory. By contrast, when non-U.S. persons conduct business that does not involve a U.S. nexus, primary sanctions do not apply.

3.2 Are parties required to block or freeze funds or other property that violate sanctions prohibitions?

U.S. persons are required to block the funds or other assets of persons listed on the SDN List and persons captured by the 50 per cent rule. Any blocked funds must be placed into separate suspense accounts and cannot be released without specific authorisation from OFAC.

The fact that a particular transaction is prohibited under OFAC regulations does not necessarily mean that it is subject to a blocking requirement. In many cases, the transaction must simply be rejected. For example, a U.S. bank would have to reject a wire transfer between two third-country companies (non-SDNs) involving an export to a non-SDN located in Syria. Because U.S. sanctions prohibit the U.S. bank from indirectly providing financial services to Syria, the bank would not be able to assist in the wire transfer.

There are also reporting requirements associated with blocked and rejected funds, as described in question 3.4.

3.3 Are there licences available that would authorise activities otherwise prohibited by sanctions?

Yes, OFAC maintains a number of exemptions and general licences under its various sanctions programmes. These exemptions and general licences can be found in OFAC’s regulations and on OFAC’s website (<https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>). For transactions or activities not expressly permitted by an exemption or general licence, parties can submit specific licence requests to OFAC.

3.4 Are there any sanctions-related reporting requirements? When must reports be filed and what information must be reported?

Generally, U.S. persons who come into possession or control of blocked property or who reject a transaction must submit a blocked property or reject report to OFAC within 10 days of blocking the property or rejecting the transaction. Holders of blocked property must also submit an annual report to OFAC detailing all blocked property in their possession.

Additionally, parties making use of certain general licences must report the specifics of such use to OFAC as required by the particular licence (e.g., annually).

3.5 How does the government convey its compliance expectations? Are certain entities required to maintain compliance programmes? What are the elements of a compliance programme required (or recommended) by the competent regulator(s)?

OFAC regularly publishes guidance and FAQs regarding sanctions restrictions and compliance expectations on its website. In addition, in May 2019, OFAC published “A Framework for OFAC Compliance Commitments”, which describes the elements of an effective sanctions compliance programme – for both U.S. and non-U.S. entities – organised around five “essential components of compliance”: (i) management commitment; (ii) risk assessment; (iii) internal controls; (iv) testing and auditing; and (v) training.

4 Enforcement

4.1 Are there criminal penalties for violating economic sanctions laws and/or regulations?

Yes, there are criminal penalties for “wilfully” violating U.S. economic sanctions laws and regulations.

4.2 Which government authorities are responsible for investigating and prosecuting criminal economic sanctions offences?

The DOJ has responsibility for the prosecution of criminal sanctions offences. The DOJ and OFAC often pursue parallel investigations, and violations can be subject to both criminal and civil penalties. State criminal authorities can also prosecute conduct related to sanctions violations (for example, sanctions-related violations of state banking laws).

4.3 Is there both corporate and personal criminal liability?

Yes. U.S. and non-U.S. corporations and individuals can be held criminally liable for violations of U.S. sanctions laws and regulations.

4.4 What are the maximum financial penalties applicable to individuals and legal entities convicted of criminal sanctions violations?

The maximum criminal fine for violations of most U.S. sanctions programmes is \$1 million or 20 years in prison for each violation. Under the Kingpin Act, certain narcotics-related sanctions violations can trigger criminal fines of up to \$5 million or 30 years in prison per violation. Funds related to sanctions violations can also be subject to criminal forfeiture. There is no statutory ceiling on the size of the total penalty or forfeiture that could be imposed, and there have been several recent criminal sanctions enforcement actions that resulted in penalties and/or forfeitures of hundreds of millions and even billions of dollars.

4.5 Are there other potential consequences from a criminal law perspective?

Yes. For example, a corporate compliance monitor can be imposed as part of a guilty plea or other resolution, such as a deferred prosecution agreement.

4.6 Are there civil penalties for violating economic sanctions laws and/or regulations?

Yes, monetary penalties can be imposed for civil violations of U.S. sanctions. Civil violations are “strict liability” offences, meaning that a person can be liable for committing a civil violation of OFAC sanctions regardless of that person’s knowledge or degree of fault.

4.7 Which government authorities are responsible for investigating and enforcing civil economic sanctions violations?

OFAC is primarily responsible for investigating and enforcing civil economic sanctions violations.

4.8 Is there both corporate and personal civil liability?

Yes. U.S. and non-U.S. corporations and individuals can be held civilly liable for violations of U.S. sanctions laws and regulations.

4.9 What are the maximum financial penalties applicable to individuals and legal entities found to have violated economic sanctions?

OFAC has the authority to impose significant civil fines. Currently, for OFAC sanctions programmes authorised under IEEPA, OFAC may impose a maximum civil fine of \$311,562 per violation. For TWEA violations (involving Cuba sanctions), the current maximum civil fine is \$91,816 per violation. Violations of the Kingpin Act are currently subject to a maximum civil fine of \$1,548,075 per violation. These amounts are subject to periodic inflation adjustments.

4.10 Are there other potential consequences from a civil law perspective?

Yes. For example, to the extent that an entity or individual found to have civilly violated sanctions laws or regulations has a specific licence from OFAC or is applying for one, OFAC may withhold, deny, suspend, modify, or revoke licence authorisations as a result of the civil violation. Where appropriate, OFAC may also refer a matter to the DOJ for criminal prosecution.

4.11 Describe the civil enforcement process, including the assessment of penalties. Are all resolutions by the competent authorities public?

OFAC may initiate an investigation of a potential sanctions law violation based on a number of sources, including press reports, leads from other agencies (domestic and international), blocking and reject reports, suspicious activity reports, voluntary self-disclosures, and “tips” from employee whistleblowers or competitors.

OFAC’s Economic Sanctions Enforcement Guidelines (the “Guidelines”) set forth the ways in which OFAC may resolve a sanctions investigation, ranging from non-public “no action” letters or cautionary letters to public civil monetary penalties or findings of violation (in which OFAC determines a violation has occurred but that imposition of a monetary penalty is not appropriate). In particularly important cases, OFAC also publicly releases the settlement agreement. The vast majority of OFAC

investigations are resolved with cautionary letters, which serve as “warnings” but refrain from determining that a sanctions violation has occurred. The Guidelines describe the “General Factors” OFAC uses in determining the appropriate enforcement action and any appropriate civil penalty.

The Guidelines also describe the process by which OFAC calculates penalty amounts. The process generally consists of three steps: first, a determination of whether the violations were “egregious” and whether they were “voluntarily self-disclosed”; second, a determination of the “base penalty” amount; and third, an upward or downward adjustment of the base penalty amount based on applicable General Factors. The General Factors include the person’s willfulness or recklessness, the person’s awareness of the conduct at issue, the harm to sanctions programme objectives, and the existence and adequacy of the person’s OFAC compliance programme. Other factors include the person’s remedial response, the person’s cooperation with OFAC, the timing of the violations in relation to the imposition of sanctions, other related enforcement actions taken by other agencies for the same or similar conduct, the impact OFAC’s enforcement response may have on promoting future compliance with U.S. sanctions by the person or similarly situated persons, and other relevant factors on a case-by-case basis, including the proportionality of OFAC’s enforcement response to the nature of the underlying conduct.

4.12 Describe the appeal process. Have companies challenged penalty assessments in judicial proceedings?

Final OFAC actions (civil penalties and findings of violation) may be challenged in federal court. These challenges proceed in the same manner and with the same standard of review as other challenges to a final agency action under relevant U.S. laws, including the Administrative Procedure Act (5 U.S.C. §§ 551–559).

4.13 Are criminal and civil enforcement only at the national level? Is there parallel state or local enforcement?

Enforcement of economic sanctions is primarily handled at the federal level; however, there are some state regulatory agencies (particularly financial services regulators such as the New York Department of Financial Services) and local prosecutors that can investigate and impose fines for violations of state laws and regulations that relate to federal sanctions violations (*e.g.*, failing to have an effective sanctions compliance programme as required by state banking laws and regulations).

4.14 What is the statute of limitations for economic sanctions violations?

The applicable federal statute of limitations is generally five years from the date of the violation.

5 General

5.1 If not outlined above, what additional economic sanctions-related measures are proposed or under consideration?

In general, there is no advance notice of the imposition of new U.S. sanctions by the President or OFAC. There are various pieces of proposed legislation involving sanctions pending in Congress.

5.2 Please provide information for how to obtain relevant economic sanctions laws, regulations, administrative actions, and guidance from the Internet. Are the materials publicly available in English?

These materials are publicly available in English on OFAC’s website (<https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx>).

Acknowledgment

The authors would like to acknowledge the assistance of associate Joshua R. Thompson who contributed to this chapter.



Roberto J. Gonzalez is a litigation partner and the co-chair of the firm's Economic Sanctions and Anti-Money Laundering Practice Group. He represents global financial institutions, technology companies and other clients in civil and criminal investigations and enforcement matters relating to U.S. economic sanctions, export controls, and anti-money laundering. He also provides regulatory advice, compliance counselling, and transactional due diligence to U.S. and non-U.S. companies across a range of sectors. He writes and speaks frequently on these topics. Roberto joined Paul, Weiss after serving several years in senior legal positions at the U.S. Treasury Department, the Consumer Financial Protection Bureau, and the White House Counsel's Office. As Deputy General Counsel of the Treasury Department, Roberto supervised over a hundred lawyers – including the legal offices of OFAC and FinCEN – in the areas of sanctions, anti-money laundering, and financial regulation. He uses his multi-faceted experience in the federal government to help clients navigate the constantly evolving U.S. regulatory and enforcement landscape.

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, D.C., 20006-1047
USA

Tel: +1 202 223 7316
Email: rgonzalez@paulweiss.com
URL: www.paulweiss.com



Rachel M. Fiorill, Counsel in the Litigation Department, formerly served as an Enforcement Section Chief at the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC").

At OFAC, Rachel led the investigation and resolution of hundreds of enforcement actions, including several groundbreaking civil monetary penalties. She served the Enforcement Division's lead for Ukraine/Russia and Syria-related investigations and developed particular expertise with OFAC's Iran sanctions while representing the Enforcement Division in agency-wide Joint Comprehensive Plan of Action ("JCPOA") implementation matters. She liaised with other law enforcement and intelligence agencies regarding joint investigations, enforcement priorities and strategies and provided guidance on OFAC's Economic Sanctions Enforcement Guidelines and sanctions programmes to counterparts at other agencies and the public.

She advises clients on government inquiries and investigations, sanctions compliance and risk management, and transactional due diligence. She counsels on a variety of financial crime and international trade issues, including economic sanctions, anti-money laundering, anti-corruption, and export controls.

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, D.C., 20006-1047
USA

Tel: +1 202 223 7346
Email: rfiorill@paulweiss.com
URL: www.paulweiss.com

Paul, Weiss is a firm of more than 1,000 lawyers with diverse backgrounds, personalities, ideas and interests who provide innovative and effective solutions. We take great pride in representing our clients in their most critical legal matters and most significant transactions, as well as individuals and organisations in need of *pro bono* assistance.

Our team advises U.S. and non-U.S. clients across industries on their most sensitive U.S. economic sanctions, export control, and Bank Secrecy Act/anti-money laundering (BSA/AML) issues. We provide regulatory advice and compliance counselling, apply for licences and interpretive guidance on behalf of clients, and perform transactional due diligence. With our preeminent regulatory defence and white collar experience, we are also uniquely positioned to: assist clients in responding to regulator inquiries, examinations, and subpoenas; conducting internal investigations; and handling matters that develop into multi-agency civil and criminal investigations.

www.paulweiss.com

Paul | Weiss

ICLG.com



Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms