# International Comparative Legal Guides

# Sanctions 2021

A practical cross-border insight into sanctions law

**Second Edition**

**Featuring contributions from:**

Blake, Cassels & Graydon LLP
BONIFASSI Avocats
BSA Ahmad Bin Hezeem & Associates LLP
De Brauw Blackstone Westbroek N.V.
Delfino e Associati Willkie Farr & Gallagher LLP
Dorda Rechtsanwälte GmbH
EY Forensic & Integrity Services
Ferrari & Associates
Gibson, Dunn & Crutcher LLP
Guidehouse
HFW
Homburger
Johnson Winter & Slattery
JunHe LLP
Kluge Advokatfirma AS
Nishimura & Asahi
Paul, Weiss, Rifkind, Wharton & Garrison LLP
Rybalkin, Gortsunyan & Partners
Schoups
Wiggin and Dana LLP
Yulchon LLC

ICLG.com

ISBN 978-1-83918-072-9
ISSN 2633-1365

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

Consulting Group Publisher
Rory Smith

Publisher
Jon Martin

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 2021

### Second Edition

Contributing Editors:
**Roberto J. Gonzalez & Rachel M. Fiorill**
**Paul, Weiss, Rifkind, Wharton & Garrison LLP**

# Expert Chapters



# Q&A Chapters

# Key Aspects of U.S. Financial Sanctions Risk for Non-U.S. Companies


Tahlia Townsend


David H. Laufman

Wiggin and Dana LLP

Since January 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), which administers most U.S. financial sanctions programmes, has imposed approximately $1.3 billion of civil penalties for violations of U.S. sanctions on non-U.S. companies or on U.S. companies based on the actions of their non-U.S. subsidiaries. The U.S. government has also imposed financial sanctions (asset freezes and inability to do any business with U.S. parties) on a significant number of foreign companies and individuals because they engaged in dealings with or for the benefit of targets of U.S. financial sanctions.

The U.S. government has repeatedly demonstrated its intent to vigorously pursue foreign parties who engage in conduct contrary to U.S. financial sanctions. In the words of Deputy Assistant Secretary of State David Peyman:

> *"[W]e are going to continue to aggressively enforce sanctions wherever a private sector or a government actor may be violating them. And we're going to look towards enforcing them in a strategic way … to send a message across [] industry."* [1]

The United States' forceful assertion of authority to enforce U.S. financial sanctions programmes against non-U.S. parties is a significant trap for the unwary, with the potential for far-reaching adverse consequences. In addition to large fines, dealings with targets of U.S. sanctions – even when completely lawful in the jurisdiction where a party operates – may: create barriers to attracting U.S. investment, doing business with U.S. companies, or investing in U.S. businesses; put companies in breach of contractual obligations to their financial institutions; or even result in the imposition of financial sanctions.

As U.S. sanctions risk continues to increase, it is critical for non-U.S. companies to understand how U.S. sanctions rules may reach their activity outside the United States, and implement internal controls to mitigate that risk. In this Chapter, we explain four key aspects of U.S. financial sanctions risk: (1) the penalties the U.S. government can impose for activities that violate U.S. financial sanctions; (2) the principal hooks through which OFAC can assert jurisdiction over activities by foreign parties outside the U.S.; (3) why even transactions with no nexus to the U.S. are not free from U.S. financial sanctions risk; and (4) how paying insufficient attention to U.S. financial sanctions risk can endanger critical relationships with banks and investors.

## 1. Penalties available to the U.S. government

The U.S. government wields some big sticks with which to punish violations of its sanctions programmes. And it casts a wide net, asserting authority to pursue administrative or criminal penalties against both U.S. and non-U.S. parties who engage in transactions that involve targets of U.S. sanctions, whenever those transactions have a nexus to the United States. As explained further below, relevant nexuses to the U.S. include use of the U.S. financial system (e.g., payment in U.S. dollars or use of accounts at a foreign branch of a U.S. bank), export or re-export of U.S. origin goods, or involvement of a U.S. citizen or permanent resident, or of a party or equipment located in the United States.

Where a U.S. nexus exists, the U.S. government may pursue administrative penalties of over $300,000 per violation for most sanctions programmes, even if the violation is unintentional. If the violation is wilful, the government may pursue criminal penalties, including fines up to $1 million per violation, and possible jail time. Moreover, enforcement actions that result in a finding of violation or imposition of a penalty are public and carry consequences well beyond the payment of fines including: triggering red flags and additional scrutiny during due diligence by prospective partners, investors, acquirors, and financiers; putting companies in breach of sanctions clauses in banking contracts; creating a disadvantage or disqualification in participation in government contracts; and attracting additional scrutiny from the Committee on Foreign Investment in the United States (CFIUS) when attempting to acquire or invest in U.S. businesses.

Where there is no U.S. nexus, the U.S. government lacks jurisdiction to pursue civil or criminal penalties against non-U.S. parties. But it nonetheless asserts authority to punish foreign entities that engage in transactions that it perceives as undermining its sanctions programmes or otherwise threatening U.S. national security or foreign policy. It does so by imposing financial sanctions directly on the offending parties, most commonly by designating them as Specially Designated Nationals and Blocked Persons (SDN), a measure that results in blocking of the listed party's property in the possession or control of U.S. parties, denial of entry to the United States, and a far-reaching prohibition on dealings with the listed party by U.S. persons: essentially ex-communication from the U.S. economy and, due to de-risking by multinational financial institutions, global economic pariah status. Further explanation of the circumstances in which the U.S. government may pursue such a course is provided in Part 3, below.

## 2. Hooks for U.S. jurisdiction over transactions outside the United States

### A. Transactions in U.S. dollars

OFAC has jurisdiction over transactions that involve parties

or activities within the United States. A critical subset of such transactions frequently overlooked by foreign parties are transactions that occur entirely outside the U.S. but involve movement of funds through a financial institution in the U.S. – i.e., almost all transactions conducted in U.S. dollars (USD).

Recent enforcement actions against foreign parties based on use of the U.S. financial system include the following:

- In April 2019, several non-U.S. UniCredit Bank subsidiaries paid OFAC a collective $600 million. One particularly interesting aspect of the enforcement involved letters of credit for USD sales of cotton and oil. The transactions were between parties that were not subject to sanctions and called for delivery of the goods to countries not subject to sanctions. The problem, according to OFAC, was that documents presented with the letters of credit showed that the purchaser of the oil intended to transfer it to a party in Iran, and the purchaser of the cotton intended to transport it to and store it in Iran en route to its final, non-sanctioned destination. Accordingly, OFAC asserted that the UniCredit banks should have known that the letters of credit had a connection to Iran and that, by instructing U.S. banks to clear dollars for the Iran-related letters of credit, the UniCredit entities violated U.S. sanctions.[2]
- In September 2019, OFAC reached a $228.8 million agreement with U.K.-based British Arab Commercial Bank (all but $4 million of which was suspended after discussions with U.K. authorities). According to OFAC, BACB directed European banks periodically to transfer large quantities of USD from BACB's EU accounts into a BACB USD account at a bank in a non-sanctioned country. The problem was that BACB used the previously-transferred USD to process customer payments involving Sudan – which at that time was subject to U.S. sanctions. Although the transfers from the U.S. pre-dated the Sudan-related payments, OFAC asserted that they corresponded exactly to each other and that by causing U.S. banks to transfer USD in order to fund Sudan-related transactions, BACB violated U.S. sanctions.[3]
- In July 2020, Essentra FZE, a UAE maker of cigarette filters and tear tape for tobacco packaging, paid OFAC $665,112 to settle allegations that Essentra exported cigarette filters to North Korea and received payments for those exports that violated U.S. sanctions either because they were denominated in USD and transited U.S. banks, or were denominated in other currencies but deposited into Essentra accounts at an overseas branch of a U.S. bank.[4]

Agreements to pay in USD for goods and services provided by and between non-U.S. parties outside the United States, and maintenance of accounts at overseas branches of U.S. banks are common and significant sources of sanctions risk for foreign businesses. Non-U.S. parties should be mindful of these bases for U.S. jurisdiction when conducting transactions that are lawful in the jurisdiction(s) where the parties operate, but could violate U.S. sanctions by involving U.S. banks in transactions that have a sanctions nexus.

Foreign parties using the U.S. financial system should also be aware that U.S. banks (and indeed all U.S. parties) have a legal obligation to report to OFAC any transaction in which a sanctions target has a blockable property interest, as well as any transaction that the U.S. party has to reject because its participation would violate U.S. sanctions. As a result, inadvertent violations by non U.S. parties may come to OFAC's attention before the parties understand or have a chance to voluntarily disclose the error (a common practice in the U.S., where regulators offer significant reductions in available penalties to parties who self-report and implement appropriate corrective measures to avoid future violations).

### B. Transactions involving goods that are subject to U.S. export controls

Transactions involving goods that are subject to U.S. export controls are also subject to U.S. jurisdiction. Such transactions pose a double risk, potentially triggering enforcement by both OFAC and the Department of Commerce, Bureau of Industry and Security (BIS), which is responsible for administering the Export Administration Regulations (EAR) (the United States' regulations governing exports of commercial, dual use, and less sensitive military items).

Like OFAC, BIS can pursue civil fines of over $300,000 per violation for inadvertent violations and recommend criminal prosecution for wilful violations. Foreign parties who transfer EAR-controlled goods to U.S. sanctions targets can also be placed on the EAR Entity List, which does not result in asset blocking but does make listed parties ineligible to receive any hardware or technology subject to the EAR.

Jurisdiction based on U.S.-controlled goods reaches much further than many foreign companies realise, for three main reasons: (1) U.S. export controls continue to apply to goods produced in the U.S. even after export, and parties in possession of such goods overseas must comply with U.S. law when transferring them to another country, end-user, or end-use; (2) U.S. export controls apply to data and software stored in the U.S., so downloads of foreign-produced software and data from, e.g., cloud services that use U.S. servers must comply with U.S. controls; and (3) U.S. export controls apply to a significant number of goods that are produced outside the U.S. but that either contain controlled U.S. content or are produced from certain U.S. software or technology.

Examples of enforcement actions against foreign parties based on transfer of U.S.-controlled goods include the following:

- In February 2020, Société Internationale de Télécommunications Aéronautiques SCRL (SITA), a Swiss provider of telecommunications and IT services to the air transportation industry, paid $8 million to settle OFAC allegations that SITA allowed its members, which included airlines subject to U.S. sanctions, to: (1) send messages to other industry parties (such as orders for aircraft maintenance and refuelling) using an application that routed the messages through switches located in the U.S.; (2) use U.S.-origin software to manage processes such as check-in and baggage management; and (3) use a global lost baggage tracing and matching system that was hosted on servers in the U.S. and also maintained by a SITA subsidiary in the United States.[5]
- In November 2019, Lebanon-based Ghaddar Machinery paid BIS $368,000 to settle allegations that Ghaddar exported, from Lebanon to Syria, foreign produced generator sets that incorporated U.S.-origin engines. Notably, Ghaddar obtained the U.S.-controlled engines from a supplier in the U.K., not the United States.[6]
- In December 2018, Shandong-based Yantai Jereh Oilfield Services Group paid $2.8 million to OFAC and an additional $600,000 to BIS. According to OFAC/BIS, Yantai obtained oilfield equipment parts from U.S. suppliers and integrated those parts into foreign produced systems that it sold to non-sanctioned parties, who transferred the systems to Iran, allegedly with Yantai's knowledge.[7]
- Since the beginning of 2019, BIS has added dozens of foreign companies to the Entity List. A frequent basis for these listings was the allegation that they transferred U.S.-origin goods to Iran or Syria.

To minimise the risk of an OFAC-BIS double punch, foreign companies should identify suppliers in the U.S. as well as suppliers outside the U.S. that provide goods produced in the U.S., or with U.S. content, or from U.S. technology. To guard against surprises, foreign companies should ask suppliers whether their products are subject to U.S. export controls, and should implement controls to monitor any such items and ensure that retransfers comply with U.S. law.

### C. Transactions involving shared services/personnel in the United States

Transactions by and between foreign parties outside the U.S. are also subject to U.S. jurisdiction if they involve personnel or equipment in the United States. Common scenarios include U.S.-based managers approving a transaction, or U.S.-based personnel providing support functions. For example:

- As detailed above, in February 2020, Geneva-based SITA paid OFAC $8 million based in part on allegations that it provided sanctioned airlines with services that included transmitting messages via telecommunications switches in the U.S., and providing access to a software platform that was maintained by an entity in the United States.
- In 2014, U.S.-based affiliates of U.K.-based health insurer Bupa entered into a $128,704 settlement with OFAC based on allegations that personnel in the U.S. transmitted policy documents, maintained policy records, and processed premium payments for health insurance policies issued to sanctioned parties by non-U.S. Bupa entities.[8]
- In 2018, Ericsson AB of Sweden (EAB) and its U.S. affiliate (EUS) paid OFAC $145,893 based on allegations that, after installing non-U.S. telecommunications equipment in Sudan, EAB arranged for EUS employees to troubleshoot problems with the equipment in Sudan and to help purchase replacement equipment from U.S. suppliers and ship it to Sudan.[9]

To limit U.S. sanctions risk, foreign companies should identify situations in which personnel in the U.S. may support non-U.S. transactions, including functions such as management approval, customer support, engineering collaboration, back office support, or maintenance of software and data platforms.

### D. Transactions involving U.S. persons outside the United States

U.S. persons (U.S. citizens, dual nationals, permanent residents, and entities organised under U.S. law) must comply with U.S. sanctions in all activities, anywhere in the world. This prohibition covers both direct and indirect involvement in transactions with sanctions targets, including referring, approving, guaranteeing, *or in any way facilitating* other parties' transactions.

In practice, enforcement actions against foreign companies based solely on the involvement of a U.S. person *outside* the United States are unusual. Enforcement based on facilitation by parties in the U.S. or the U.S. financial system, or transfer of U.S.-controlled goods are much more common. Nonetheless, the involvement of U.S. persons outside the U.S. is a risk factor, both because it can create jurisdiction and because, if OFAC has jurisdiction on other grounds, it may count facilitation by U.S. persons outside the U.S. as additional violations or as an aggravating factor in setting penalties.

To take one example, in July 2020, U.S.-based cookware coating manufacturer Whitford Worldwide paid $824,314 to settle allegations that its Italian and Turkish subsidiaries sold cookware coatings to Iran. OFAC had jurisdiction because the Iranian Transactions and Sanctions Regulations require foreign companies owned by U.S. persons to comply with the Iran embargo. However, OFAC also cited as independent and additional violations, and as an aggravating factor in determining the penalty, the facilitation of the Iran sales by Whitford's U.S.-person Managing Director for Europe.

For the reasons above, before pursuing business opportunities that are lawful under local law but in tension with U.S. sanctions programmes, foreign companies should identify board members, directors, employees, or contractors who are U.S. persons. Such persons must be excluded from any involvement in transactions that involve a U.S. sanctions target. However, even the process of exclusion can raise difficult questions of sanctions law, so companies facing such situations should seek legal advice before proceeding.

### E. U.S. ownership or control of foreign businesses

Foreign businesses owned or controlled by U.S. persons generally are not legally required to comply with U.S. sanctions, provided that no other hooks for U.S. jurisdiction exist. However, U.S. sanctions regulations on *Iran* and *Cuba* expressly require compliance by U.S.-owned/controlled foreign parties.

U.S.-owned/controlled foreign companies' failure to comply with U.S. Iran and Cuba sanctions has been the focus of a number of recent enforcement actions. Importantly, OFAC will pursue such actions even when the jurisdiction in which the foreign company operates maintains blocking statutes that prohibit compliance with the U.S. embargoes (e.g., Canada and the European Union). Companies operating in such jurisdictions should be aware that the existence of such laws does not provide a defence to OFAC enforcement, and should seek legal advice on how to address the conflict of law.

Representative recent enforcement actions include the following:

- In February 2019, AppliChem of Germany paid OFAC $5,512,564 to settle allegations that, after being acquired by a U.S. company, it continued to fill orders for pre-existing Cuban customers and hid those activities from its U.S. parent using tactics such as referring to Cuba by the code word "Caribbean".[10]
- In March 2019, Stanley Black & Decker paid $1,869,144 to settle allegations that a Chinese subsidiary continued to export goods to Iran after Stanley's acquisition. According to OFAC, the subsidiary concealed its Iran sales from Stanley by using trading companies in China and the UAE as conduits, instructing customers not to write "Iran" on business documents, and creating fictitious bills of lading.[11]
- In April 2019, U.K.-based Acteon Group paid $227,000 over allegations that Malaysian affiliates performed oil well drilling-related services in Cuban waters. OFAC had jurisdiction because, at the time, Acteon was majority-owned by funds associated with a U.S. investment firm. Simultaneously, OFAC reached a $213,866 settlement with Acteon and another U.S. investment company, which had acquired control after the above-referenced violations. The second settlement involved allegations that Acteon subsidiaries in the U.S., Singapore, and UAE transferred equipment to third parties who Acteon knew or should have known embarked the equipment on vessels in Cuban or Iranian territorial waters, and sent company engineers to service such equipment on vessels in Cuban waters.[12]

Foreign companies contemplating investment from U.S. companies should be prepared to undergo stringent due diligence and to immediately terminate business involving Cuba/Iran upon U.S. acquisition/control. U.S-owned companies in jurisdictions with blocking statutes prohibiting compliance with certain U.S. sanctions should understand that those statutes do not provide a defence to OFAC enforcement and should seek legal advice on handling the conflict of laws.

## 3. Even when the U.S. lacks jurisdiction, it punishes parties that undermine its sanctions programmes' goals

When non-U.S. parties engage in transactions with no nexus to the United States, one might imagine that it would be unnecessary to consider whether the transactions involve a U.S. sanctions target. But that is not the case.

To the contrary, the U.S. has made steadily increasing use of so-called "secondary sanctions" to enforce its sanctions goals even where it lacks jurisdiction, imposing financial sanctions on foreign parties who are not engaged in the primary activities targeted by U.S. sanctions programmes (e.g., terrorism, narcotics trafficking, corruption, human rights abuses, etc.), but who engage in dealings with parties or countries that are subject to U.S. sanctions.

A majority of U.S. sanctions programmes contain language authorising the Secretary of Treasury to impose financial sanctions on parties who "materially assist, sponsor, or provide financial, material, or technological support for, or goods or services in support of", parties on whom financial sanctions have been imposed under that programme. The U.S. government uses these provisions sparingly with respect to transactions involving parties blocked under most of its sanctions programmes, typically only targeting foreign parties who directly facilitate the primary activities targeted by the programme (e.g., terrorism, corruption) or who help the sanctions target to evade U.S. sanctions (for example, by setting up front companies to transfer funds or obtain goods or services for the sanctions target).

However, with respect to U.S. sanctions programmes targeting Iran, Syria, North Korea, Russia and Venezuela, the U.S. government has clearly stated its intention to vigorously pursue secondary sanctions, and foreign parties face the risk of becoming subject to sanctions for a wide variety of activity involving targets of these sanctions programmes, including for certain dealings with or for: the Iranian banking, construction, energy, finance, insurance, petroleum, petrochemical, shipping, shipbuilding, graphite and coal, iron, steel, aluminum, copper, gold and precious metals, mining, manufacturing, and textile sectors, and parties sanctioned under various Iran-related authorities; the Syrian defence and energy sectors and Syrian government entities; the Russian energy, defence, and intelligence sectors, and parties sanctioned under Russia/Ukraine authorities; the North Korean energy, financial services, fishing, manufacturing, mining, and transport sectors; and the Venezuelan gold, oil, finance, defence and security sectors.

Recent years have seen a significant uptick in foreign parties being subject to asset-blocking sanctions for dealings with U.S. sanctions targets. Fox example, in August 2018, Treasury sanctioned Russian port service agency Profinet for providing port services to DPRK-flagged vessels. In September 2019, the U.S. sanctioned two subsidiaries of China's largest shipping company, COSCO, and several other companies and their executives, for transporting Iranian oil. In January 2020, Treasury sanctioned multiple companies in China, Hong Kong and the UAE for allegedly buying and selling steel and cathode blocks from/to Iranian metals producers, transporting Iranian metal products, and facilitating shipments of Iranian petrochemicals. And in spring 2020, the U.S. sanctioned two Swiss subsidiaries of Russia's Rosneft for allegedly purchasing large quantities of crude oil from Venezuela.

Non-U.S. parties should be aware that, even when lawful in their countries of operation, and even when there is no U.S. nexus, dealings with U.S. sanctions targets carry an increasing risk that the U.S. will punish the transaction parties with asset-blocking sanctions. Foreign parties would be well-advised to implement controls to identify transactions that may involve U.S. sanctions targets and defer them pending careful evaluation of the secondary sanctions risk, as well as potential risks to banking, investor, and customer relationships.

## 4. Financial institutions and the privatisation of OFAC enforcement

The U.S. government has imposed billions of dollars of penalties on major U.S. and foreign financial institutions for processing and/or causing U.S. banks to process funds related to transactions involving sanctions targets. As a result, banks worldwide have implemented customer due diligence procedures to identify customers whose business may present sanctions risk, screening software that checks transaction data for red flags indicating a connection to a sanctions target, and other tools to prevent their customers from exposing them to sanctions risk.

Among other risk-management tools, both U.S. and non-U.S. banks frequently include sanctions compliance clauses in master service agreements, overdraft facilities, and credit agreements. These clauses range in breadth, but may require the customer to certify that neither they nor their affiliates do any business with countries, regions, or parties that are subject to U.S. sanctions. Often, these clauses go further than the law requires, requiring compliance by parties not normally subject to U.S. jurisdiction, and/or prohibiting transactions involving U.S. sanctions targets even when such transactions could be lawfully conducted under a regulatory exception or licence.

Similarly, many banks require customers to complete annual "Know Your Customer" (KYC) questionnaires that include detailed sanctions-related questions. If a banking customer or its affiliates disclose activities involving sanctions targets, the bank may ask numerous and intrusive follow-up questions and/or demand that the customer take steps to prevent any "tainted" funds passing through the bank, and/or conclude that the customer presents too much risk, and ask the customer to close its accounts. Where customers fail to disclose sanctions-related activity, and such activity comes to the bank's attention by other means, banks may assert breach of contract and/or direct the customer to bank elsewhere.

Inaccurate completion of KYC questionnaires and breach of sanctions clauses can create significant problems in banking relationships. To minimise risk, companies should ensure that they know what the sanctions clauses in their banking agreements say, and that the personnel who sign such contracts and process banks' KYC questionnaires communicate early and often with company compliance personnel and others knowledgeable about activities involving sanctions targets.

Foreign companies should note that public records connecting a company to a sanctions target, even with respect to lawful business, may generate red flags in the automated screening processes used by banks and that banks may temporarily block payments and other transactions involving the company while investigating whether such red flags are significant. While these situations can often be resolved through dialogue with the bank, they can create tremendous short-term disruption and harm the

company's reputation with parties whose payments are held up during the bank's investigation.

Finally, foreign companies should be aware that U.S. sanctions risk is a matter of increasing concern to investors and acquirors (both U.S. and non-U.S.), and that committing sanctions violations or conducting lawful business involving sanctions targets can introduce significant complexity into investment and M&A activity.

* * *

U.S. financial sanctions pose complex and significant risks for foreign parties. Understanding how U.S. financial sanctions can reach activity outside the United States and implementing internal controls to address that risk has never been more essential. As Deputy Assistant Secretary of State Peyman explained in a March 2020 speech at the Foundation for Defense of Democracies:

> *"The clear message that … we're trying to send … is that no company is too big to fail when it comes to protecting US national security. No company is too safe," "[i]n the first three years of this administration, we've had close to 800 [sanctions designation] actions. We expect this pace to continue."*

## Endnotes

1. Transcript of comments at the Foundation for Defense of Democracies (2020).
2. *See* UniCredit settlements (April 2019) available at https://home.treasury.gov/news/press-releases/sm658.
3. *See* BACB settlement (Sept. 2019) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190917_bacb.pdf.
4. *See* Essentra settlement (June 2020) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20200716_essentra_fze.pdf.
5. *See* SITA settlement (Feb. 2020) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20200226_sita.pdf.
6. *See* BIS order re Ghaddar Machinery (Nov. 2019) available at https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=1253&Itemid=.
7. *See* Yantai Jereh settlement with OFAC (Dec. 2018) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20181212_jereh.pdf. *See also* concurrent settlement with BIS available at https://efoia.bis.doc.gov/index.php/component/docman/?task=doc_download&gid=1207&Itemid=.
8. *See* Bupa settlement (Oct. 2014) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20141029_bupa.pdf.
9. *See* Ericsson settlement (June 2018) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20180606_ericsson.pdf.
10. *See* AppliChem settlement (Feb. 2019) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190214_applichem.pdf.
11. *See* Stanley settlement (March 2019) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190327_decker.pdf.
12. *See* Acteon and KKR settlements (April 2019) available at https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190411_acteon_webpost.pdf.

**Tahlia Townsend**, co-chair of the International Trade Compliance practice at Wiggin and Dana LLP, is an experienced, Chambers-recognised financial sanctions, export controls, and foreign investment attorney known for providing insightful, practical and timely guidance. Trusted by U.S. and international clients from global aerospace companies and international financial institutions to top tier universities and hi-tech start-ups, Tahlia assists with government-directed and internal investigations, M&A and investment due diligence, CFIUS assessments and approvals, commodity classification and export licence applications, and building and auditing compliance programmes. Tahlia graduated from Yale Law School and clerked for two judges of the United States District Court. Before becoming a lawyer, Tahlia studied physics and chemistry, performed research in the Computer Science Department at Carnegie Mellon University, taught at the Lauder Javne Jewish community school in Budapest, Hungary, worked with an ecologist in the Serengeti, and studied French, German, and Hungarian.

**Wiggin and Dana LLP**
800 17th Street NW
Suite 520
Washington, D.C. 20006
USA

Tel: +1 202 800 2473
Email: ttownsend@wiggin.com
URL: www.wiggin.com

**David H. Laufman** is a partner at Wiggin and Dana LLP, where he serves as co-chair of the firm's National Security Practice Group, a member of its White Collar Defense, Investigations and Corporate Compliance Practice Group, and a member of its International Trade Compliance Practice Group. Mr. Laufman conducts internal corporate investigations and represents parties in federal criminal investigations and other enforcement actions, as well as in congressional investigations, Inspector General investigations, and sensitive national security matters. He also counsels clients on compliance with the Foreign Agents Registration Act, U.S. export control and sanctions laws, the Foreign Corrupt Practices Act, and government ethics laws. Mr. Laufman's practice leverages his prior experience at the Department of Justice, where he served as Chief of Staff to the Deputy Attorney General, Chief of the Counterintelligence and Export Control Section, and Assistant U.S. Attorney for the Eastern District of Virginia.

**Wiggin and Dana LLP**
800 17th Street NW
Suite 520
Washington, D.C. 20006
USA

Tel: +1 202 800 2477
Email: dlaufman@wiggin.com
URL: www.wiggin.com

Wiggin and Dana is a full-service law firm with over 140 highly talented, creative, and experienced lawyers widely recognised by Chambers, Best Lawyers, Legal 500 U.S., and IFLR 1000. With offices in Connecticut, New York, Philadelphia, Washington, D.C., and Palm Beach, we represent U.S. and international clients throughout the United States on a wide range of complex and sophisticated matters. From "bet-the-company" litigation, to helping bring a new technology to market, to preserving the wealth a family business worked hard to create, we pride ourselves on offering practical, value driven solutions. Our international trade group combines decades of government and in-house experience to deftly guide companies through the maze of U.S. export, financial sanctions, foreign investment, and anti-corruption laws, build practical compliance programmes, obtain ITAR, EAR, and OFAC licences, conduct M&A due diligence, obtain CFIUS approval, successfully navigate government and internal investigations, and defend against criminal charges.

**www.wiggin.com**

# 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
Outsourcing
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
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group