Global Investigations Review

The Guide to Sanctions

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

Second Edition

The Guide to Sanctions

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

Editors

Rachel Barnes

Paul Feldberg

Nicholas Turner

Anna Bradshaw

David Mortlock

Anahita Thoms

Rachel Alpert

GIR
Global Investigations Review

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

www.globalinvestigationsreview.com

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

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

ISBN 978-1-83862-596-2

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

Acknowledgements

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

BAKER & HOSTETLER LLP

BAKER MCKENZIE

BARNES & THORNBURG LLP

BDO USA LLP

CARTER-RUCK SOLICITORS

CRAVATH, SWAINE & MOORE LLP

EVERSHEDS SUTHERLAND

FORENSIC RISK ALLIANCE

GLOBAL LAW OFFICE

JENNER & BLOCK LLP

MCGUIREWOODS LLP

MAYER BROWN

MILLER & CHEVALIER CHARTERED

PETERS & PETERS SOLICITORS LLP

SEWARD & KISSEL

SIMMONS & SIMMONS LLP

STEPTOE & JOHNSON

STEWARTS

THREE RAYMOND BUILDINGS

WHITE & CASE LLP

WILLKIE FARR & GALLAGHER LLP

Publisher's Note

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

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

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

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

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

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

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

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

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

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

David Samuels
Publisher, GIR
June 2021

Contents

Foreword

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

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

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

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

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

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

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

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

Part III

Sanctions in Practice

20

Practical Issues in Cyber-Related Sanctions

Brian Fleming, Timothy O'Toole, Caroline Watson, Manuel Levitt and Mary Mikhaeel[1]

Development of US cyber-related sanctions regimes

Overview of the Cyber-Related Sanctions Program

The United States has been at the forefront of establishing a cyber-focused economic sanctions regime,[2] which is primarily administered by the US Department of the Treasury, Office of Foreign Assets Control (OFAC), although criminal prosecutions for certain wilful sanctions violations are the responsibility of the US Department of Justice.

OFAC administers a variety of sanctions targeting malicious cyber-related activities, such as cyberespionage, cyber-intrusions on critical infrastructure and computer networks, and disinformation campaigns conducted from abroad. The bulk of these sanctions are administered under OFAC's 'Cyber-Related Sanctions Program', which was established in 2015 as part of the Obama administration's response to malicious cyber-enabled activities originating from foreign countries that were directed at both US government agencies and private sector US entities. However, sanctions targeting malicious cyber-related activities are also authorised under other statutory and executive branch sanctions authorities, including the Countering America's Adversaries Through Sanctions Act (CAATSA), as well as Executive Order (EO)

1 Brian Fleming and Timothy O'Toole are members, Caroline Watson is a senior associate and Manuel Levitt and Mary Mikhaeel are associates at Miller & Chevalier Chartered.

2 Other jurisdictions, including the EU and UK, have begun taking significant steps to develop sanctions programmes to deter malicious cyber actors and respond to increasingly frequent and severe cyberattacks. See Council Decision 2019/797 2019 O.J. (L. 129/13) (EU); Council Regulation 2019/796 2019 O.J. (L. 129/1) (EU). See generally the Cyber (Sanctions) (EU Exit) Regulations 2020, www.legislation.gov.uk/uksi/2020/597/contents/made. While these developments are significant, the EU and UK have used sanctions far less frequently than the United States, with just eight persons and four entities sanctioned under the EU's cyber-related sanctions framework thus far. See Council Decision 2020/1127, 2020 O.J. (L 246/12) (EU); European Commission Press Release, 'Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack' (22 October 2020), www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/.

14024, Blocking Property With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation, issued on 15 April 2021.

Prior to the Obama administration's first EO authorising cyber-related sanctions, malicious cyber-intrusions and cyberespionage from abroad were becoming increasingly frequent and severe. For example, on 19 May 2014, in its first major prosecution against a state actor for malicious cyber-enabled activities, the US Department of Justice indicted five Chinese nationals, allegedly affiliated with the Chinese military, for gaining unauthorised access to computer networks for the apparent purpose of engaging in economic espionage targeted at six US entities involved in the nuclear power, metals and solar products industries.[3] In September of 2014, President Obama said his administration viewed cyber-enabled theft of trade secrets as 'an act of aggression that has to stop' and warned that the US was prepared to impose countervailing actions 'to get [China's] attention'.[4]

Prior to the establishment of OFAC's cyber-related sanctions programme, US law enforcement agencies had legal authorities available to pursue charges against individuals engaged in various types of cyber espionage or unauthorised intrusions into US government and private sector computers and networks.[5] Nevertheless, facing an increasingly severe threat posed by foreign-based hackers targeting valuable US intellectual property and sensitive private data, among other things, US national security agencies viewed sanctions as a tool well-designed to address the extraterritorial nature of cyber-enabled attacks from foreign actors.

This culminated on 1 April 2015 when President Obama issued EO 13694, which declared a national emergency to deal with 'the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States constituted by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States'.[6] As with most US economic sanctions authorities, this EO was issued pursuant to the International Emergency Economic Powers Act (50 USC §§ 1701–1708) and the National Emergencies Act (50 USC §§ 1601, 1621–1631, and 1641).

On 28 December 2016, President Obama issued EO 13757, which amended EO 13694 to broaden the scope of cyber-related activities subject to sanctions. As amended, those EOs permit the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose blocking sanctions[7] on persons determined:

- *to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in*

3 Press Release, US Dep't of Justice, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage' (19 May 2014), www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

4 Graham Webster, 'Obama: Cyber Theft 'an Act of Aggression' but US and China Can Develop Norms', *The Diplomat* (18 September 2015), https://thediplomat.com/2015/09/obama-cyber-theft-an-act-of-aggression-but-us-and-china-can-develop-norms/.

5 Computer Fraud and Abuse Act, 18 USC § 1030; Economic Espionage Act of 1996, 18 U.S.C. 1831 et seq.

6 EO No. 13,694, 80 Fed. Reg. 18,077 (1 April 2015), reprinted as amended in 22 USC § 9522.

7 Persons blocked pursuant to EO 13,694, as amended by EO 13,757, are included on the Specially Designated Nationals and Blocked Persons (SDN) List maintained by OFAC. The initial designations under this authority were made on 28 December 2016.

substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:

- *harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;*
- *significantly compromising the provision of services by one or more entities in a critical infrastructure sector;*
- *causing a significant disruption to the availability of a computer or network of computers;*
- *causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or*
- *tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; and*

- *. . . to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States;*
- *to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, [certain activities described above] or any person whose property and interests in property are blocked pursuant to [EO 13694, as amended;*
- *to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked [pursuant to EO 13694, as amended]; or*
- *to have attempted to engage in any of the activities described in [EO 13694, as amended].*[8]

Cyber-related sanctions under CAATSA

On 2 August 2017, President Trump signed into law CAATSA, which authorised, inter alia, the imposition of cyber-related sanctions targeting Russia and codified the cyber-related sanctions imposed through EO 13694 and EO 13757.[9] On 20 September 2018, President Trump issued EO 13849, 'Authorizing the Implementation of Certain Sanctions Set Forth in the Countering America's Adversaries Through Sanctions Act (CAATSA)', which delegates authority to impose sanctions under CAATSA to the Secretary of the Treasury.[10]

8 EO No. 13,757, 82 Fed. Reg. 1, 1–2 (28 December 2016).

9 22 USC § 9524. OFAC has since promulgated cyber-related sanctions regulations at 31 CFR Part 578.

10 EO No. 13,849, 83 Fed. Reg. 48,195 (20 September 2018).

With respect to Russia, section 224 of CAATSA included additional sanctions provisions targeting malicious cyber activities that are distinct from OFAC's 'Cyber-Related Sanctions Program.' Specifically, Section 224(a)(1) of CAATSA requires the President to impose blocking sanctions on any person that the President determines '(A) knowingly engages in significant activities undermining cybersecurity against any person, including a democratic institution, or government on behalf of the Government of the Russian Federation; or (B) is owned or controlled by, or acts or purports to act for or on behalf of, directly or indirectly' such person.[11] 'Significant activities undermining cybersecurity' include:

- *significant efforts:*
  - *to deny access to or degrade, disrupt, or destroy an information and communications technology system or network; or*
  - *to exfiltrate, degrade, corrupt, destroy, or release information from such a system or network without authorization for purposes of:*
    - *conducting influence operations; or*
    - *causing a significant misappropriation of funds, economic resources, trade secrets, personal identifications, or financial information for commercial or competitive advantage or private financial gain;*
- *significant destructive malware attacks; and*
- *significant denial of service activities.*[12]

Additionally, the President is required to impose five or more menu-based sanctions on persons the President determines knowingly 'materially assists, sponsors, or provides financial, material, or technological support for, or goods or services (except financial services)' in support of, the cyber-related activity described in CAATSA section 224(a)(1).[13] Those menu-based sanctions include, among others, restrictions on a sanctioned person's ability to participate in, conduct or obtain: US export licences; loans or assistance from certain US and foreign financial institutions, including the US Export-Import Bank; certain foreign exchange transactions; various transactions involving property in the United States; or US visas.[14]

For a person the President determines 'provides financial services' in support of the cyber-related activities described in CAATSA Section 224(a)(1), CAATSA requires the President to impose three or more menu-based sanctions, described separately at 22 USC § 8923.[15] These include many of the same types of sanctions mentioned above.

Cyber-related sanctions under the new EO targeting harmful foreign activities of Russia

On 15 April 2021, President Biden issued EO 14024, 'Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation', which is aimed at countering a wide array of malign Russian government-sponsored activities,

11 22 USC § 9524(a)(1).
12 id. § 9524(d)(1)–(3).
13 id. § 9524(a)(2).
14 22 USC § 9529.
15 22 USC § 9524(a)(3).

including interference in the 2020 US presidential election and the SolarWinds cyberattack, among others.[16] EO 14024 significantly expands the categories of Russian persons that can be targeted for sanctions by the United States, and includes, among others, persons determined 'to be responsible for or complicit in, or to have directly or indirectly engaged or attempted to engage in . . . malicious cyber-enabled activities'.[17] Sanctions may also be imposed under EO 14024 on the spouses and adult children of persons subject to sanctions under this EO, as well as those determined by the Secretary of the Treasury, in consultation with the Secretary of State, to have materially assisted, sponsored, or provided financial, material or technological support for, or goods or services to or in support of, among other things, malicious cyber-enabled activities.

OFAC Ransomware Advisory

On 1 October 2020, OFAC issued its 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (the Ransomware Advisory) to highlight the sanctions compliance risks associated with facilitating ransomware payments related to malicious cyber-enabled activities (e.g., by providing cyber insurance, digital forensics and incident response, and financial services related to processing ransom payments including by depository institutions and money services businesses).[18] OFAC warns that facilitating a ransomware payment may not only enable and embolden criminals, as well as adversaries with a nexus to a sanctioned party or country, but, critically, may not guarantee that a victim regains access to stolen data.

The Ransomware Advisory also notes that victims of a ransomware attack should: contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus; and contact the US Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a US financial institution or may cause 'significant disruption to a firm's ability to perform critical financial services'.

OFAC enforcement and recent illustrative cases

OFAC's use of cyber-related sanctions authorities appears to be on the rise. OFAC enforcement of these sanctions authorities generally can be divided in two parts:

- the imposition of blocking or menu-based sanctions on individuals and entities for engaging in sanctionable activities (e.g., perpetrating cyber-attacks or materially assisting by laundering funds obtained thereby); and
- the imposition of civil penalties for the violation of sanctions (e.g., transacting with a blocked person sanctioned for malign cyber activities). Criminal prosecutions for sanctions violations, which typically focus on the most egregious wilful misconduct, are within the purview of the US Department of Justice.

Since 2015, OFAC has designated numerous parties under the cyber-related sanctions authorities each year. However, OFAC has imposed relatively few civil penalties connected to cyber-related sanctions or other cyber-related sanctions compliance failures. Nevertheless,

16 EO 14,024, 86 Fed. Reg. 20,249 (19 April 2021).

17 id.

18 OFAC, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments' (1 October 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

based on recent guidance, issued in 2020, and its recent imposition of civil penalties against certain internet-based businesses and entities involved in the use of digital currencies,[19] OFAC has demonstrated that it expects parties to implement full-fledged risk-based sanctions compliance programmes to address malign cyber activities and other cyber-related vulnerabilities.

Cyber-related sanctions designations

OFAC has designated numerous persons under its cyber-related sanctions programme over the past few years, making the most such designations in 2020. Persons designated under these authorities include individual hackers, money launderers, non-state actors such as organised 'troll farms' (e.g., Internet Research Agency) and international cybercriminal organizations (e.g., Evil Corp), and even a few foreign government agencies (e.g., Russian Federation Federal Security Service). OFAC has mainly focused on actors residing in or associated with foreign nation-states perceived as hostile to the United States – primarily, Russia, China, Iran and North Korea – and engaging in certain malicious cyber-enabled activities, such as:

- development and distribution of malware, ransomware, and phishing and spoofing scams;
- interference with electoral processes and institutions worldwide through false information or hacking;
- theft of economic resources, trade secrets, personal identifying information or financial information by cyber intrusions for private financial gain;
- publication of stolen sensitive documents obtained and sometimes manipulated through cyber intrusions;
- disruption of network access; and
- compromise of US government entities and US critical infrastructure sectors.

OFAC civil penalties

To date, OFAC has not imposed any publicly disclosed civil penalties specifically tied to cyber-related sanctions violations. However, the following civil settlements generally illustrate OFAC's compliance expectations in the cyber and digital areas. A constant theme is the offending company's failure to apply relevant knowledge in its possession – particularly internet protocol (IP) addresses – to identify, prevent or block prohibited users or transactions.

- On 29 April 2021, as part of a global resolution with the US Departments of Justice, Treasury, and Commerce, the German-based software company SAP SE (SAP) entered into a settlement with OFAC to address 190 apparent violations of the US sanctions against Iran.[20] Those apparent violations arose from SAP's exportation of software and related services from the United States to companies in third countries with knowledge or reason to know the software or services were intended specifically for Iran, as well as from the sale of cloud-based software subscription services accessed remotely through SAP's cloud businesses in the United States to customers that made the services available to

19 OFAC defines 'digital currency' to include 'sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency.' OFAC, 'FAQ 559' (19 March 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.

20 OFAC, 'Enforcement Release: April 29, 2021' (hereinafter the '*SAP* Settlement') (29 April 2021), https://home.treasury.gov/system/files/126/20210429_sap.pdf.

their employees in Iran. The software deliveries were made through third countries, which then allowed customers in Iran to access US-based databases and services. This occurred despite multiple audits noting a major gap in SAP's sanctions compliance system – namely that SAP did not screen customers' Internet Protocol (IP) addresses, resulting in SAP's inability to identify the country in which SAP software was downloaded. A later SAP internal investigation revealed that SAP software was being downloaded by users in Iran. Additional potential violations occurred when SAP's subsidiaries in the United States sold cloud-based software subscription services to customers that enabled access to employees or customers in Iran. These exports occurred partly as a result of a failure to timely integrate the newly-acquired CBG subsidiaries into SAP's broader compliance structure. The SAP enforcement action highlights for global companies providing software products online, including through cloud-based services, direct downloads, or other such means: 'the importance of implementing a risk-based sanctions compliance program commensurate with their size and sophistication and appropriate to their marketing and operational structures'. US regulators also made clear that, in the area of cyber-enabled services where engagement with the end-user is often indirect, appropriate sanctions screening processes will generally include IP address identification and blocking capabilities.

- On 30 December 2020, the US-based technology company BitGo Inc. (BitGo) settled 183 apparent violations of multiple sanctions regimes for its failure to use IP addresses in its possession to prevent persons located in sanctioned jurisdictions from opening accounts and sending digital currencies via its digital wallet[21] platform.[22] While BitGo had previously allowed users to open accounts without providing any location information, beginning in 2018 BitGo relied on user attestations regarding their location but did not perform additional verification of the users' locations. This continued even after BitGo began tracking users' IP addresses for security purposes related to account logins. In the settlement, one of BitGo's mitigating measures included the implementation of IP address blocking as well as email-related restrictions for sanctioned jurisdictions.
- On 18 February 2021, the US-based company BitPay Inc. (BitPay), a digital currency payment service provider, settled 2,102 apparent violations of multiple sanctions programmes for allowing persons in sanctioned jurisdictions to transact with merchants in the United States and elsewhere in digital currency on its platform even when BitPay possessed the users' location information including IP addresses.[23] Thus, although BitPay received certain information about the buyer at the time of a transaction on its platform,

21 OFAC defines a 'digital currency wallet' as 'a software application (or other mechanism) that provides a means for holding, storing, and transferring digital currency. A wallet holds the user's digital currency addresses, which allow the user to receive digital currency, and private keys, which allow the user to transfer digital currency. The wallet also maintains the user's digital currency balance. A wallet provider is a person (individual or entity) that provides the software to create and manage wallets, which users can download. A hosted wallet provider is a business that creates and stores a digital currency wallet on behalf of a customer. Most hosted wallets also offer exchange and payments services to facilitate participation in a digital currency system by users.' OFAC, 'FAQ 559', *supra* note 19.

22 OFAC, 'Enforcement Release: December 30, 2020' (hereinafter the '*BitGo* Settlement') (30 December 2020), https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.

23 OFAC, 'Enforcement Release: February 18, 2021' (hereinafter the '*BitPay* Settlement') (18 February 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf.

including IP addresses in transactions after 2017, BitPay's process did not fully analyse this information for compliance purposes. Consequently, BitPay processed digital currency payments from buyers in sanctioned jurisdictions, converted the digital currency to fiat currency, and then relayed the payments to the sellers. As part of the settlement, BitPay implemented numerous mitigation measures, including (1) blocking IP addresses originating from sanctioned jurisdictions that attempt to connect to the BitPay website or view instructions on how to make payments; and (2) launching a new customer identification tool, BitPay ID, for transactions worth US$3,000 or more that requires the buyer to provide an email address, proof of identification and a selfie photo.

In its announcements of the *BitGo* and *BitPay* settlements, OFAC emphasised that US persons involved in the provision of digital currency services (including companies that facilitate or engage in online commerce or process transactions in digital currency) – like all other US persons – have 'sanctions compliance obligations'. Additionally, citing the essential components of compliance in its 'Framework for OFAC Compliance Commitments', OFAC highlighted the 'importance of implementing technical controls, such as sanctions list screening and IP blocking mechanisms, to mitigate sanctions risks in connection with digital currency services'.[24]

Cyber-related sanctions compliance risks

Ransom payments

As discussed in OFAC's 2020 Ransomware Advisory, a compliance risk unique to cyber-related sanctions relates to ransomware attacks, specifically the payment of ransoms themselves.[25] Unless OFAC grants a specific licence, a person who makes ransom payments to sanctioned parties or jurisdictions may face penalties for violating OFAC sanctions regulations. Particularly for ransom payments made in a digital currency, the difficulty of definitively determining whether the transaction involves a sanctioned party or sanctioned jurisdiction can create serious compliance challenges. Although no public civil penalty has been announced in connection with this type of violation, OFAC has emphasised the risks related not only to direct payments of ransoms in contravention of sanctions regulations, but also facilitating such payments (e.g., ransomware insurance businesses, payment processors).

Digital currency sector

Via its enforcement actions and guidance,[26] OFAC also has been clear that transactions and services involving digital currency present sanctions compliance risk. Thus, businesses that allow digital currency payments or that are involved in the digital currency market or sector (e.g., digital currency trading platforms, asset management, security) may need to

24 *BitGo* Settlement at 3; *BitPay* Settlement at 3.

25 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments', *supra* note 18.

26 OFAC has also periodically released Frequently Asked Questions (FAQs) addressing various topics relating to cyber-related sanctions and digital currency compliance issues more broadly. See OFAC, 'Cyber Sanctions FAQs', https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546 (accessed 3 May 2021); OFAC, 'Virtual Currency FAQs', https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626 (accessed 3 May 2021).

consider how to implement appropriate risk-based compliance measures that address the specific vulnerabilities of digital currency. Without appropriate compliance measures, a digital currency service provider could incur liability not only for violating sanctions (e.g., by dealing with blocked persons or persons in sanctioned jurisdictions), but also for facilitating sanctions violations by other parties to a transaction (even if inadvertent).

For example, just as with fiat currency, businesses involved in digital currency transactions would be expected to deploy risk-based sanctions screening for parties involved and to ensure that the funds are not destined for a sanctioned jurisdiction.[27] As described above, recent enforcement actions highlight OFAC's expectation that internet-based businesses should use all relevant known information in the course of their business for sanctions compliance purposes as well. Specifically, OFAC has recently imposed civil penalties on multiple businesses that knew customers' IP addresses (e.g., by their use of internet services) but did not ensure that customers with IP addresses in sanctioned jurisdictions were screened or blocked from using their services or transacting on their platforms.[28]

Cryptocurrency, a type of digital currency reliant on cryptography to secure and verify transactions, also presents risk because cybercriminals and other sanctioned parties (including the government of North Korea) may resort to using cryptocurrency as a tool to evade sanctions, launder money and facilitate other illegal activities (e.g., nuclear weapons proliferation[29]).[30] The proceeds of malicious cyber activities are regularly transferred to cryptocurrency exchanges and peer-to-peer marketplaces with negligible customer screening compliance programmes, or individual peer-to-peer or over-the-counter traders operating on exchanges that do not screen their customers.[31] More broadly, digital currency infrastructure has been targeted by some cybercriminals, who use illegitimate websites and malicious software to conduct phishing attacks on the digital currency sector.[32] Due diligence and controls to determine whether digital currency has been tainted by sanctionable or criminal cyber activity may be needed in certain transactions or businesses. Relatedly, OFAC has emphasised how anti-money laundering and combating the financing of terrorism controls play a vital role in sanctions and law enforcement generally because these can force cybercriminals to take measures to circumvent such controls that leave trails of evidence and traceability.[33] OFAC has begun a practice of identifying certain digital currency addresses[34] associated with

27 OFAC, 'Virtual Currency FAQ 560' (19 March 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/560.

28 See SAP Settlement, BitGo Settlement, and BitPay Settlement.

29 Michelle Nichols & Raphael Satter, 'UN experts point finger at North Korea for $281 million cyber theft, KuCoin likely victim', *Reuters* (9 February 2021), https://www.reuters.com/article/us-northkorea-sanctions-cyber/u-n-experts-point-finger-at-north-korea-for-281-million-cyber-theft-kucoin-likely-victim-idUSKBN2AA00Q.

30 See Press Releases, OFAC, 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses' (28 November 2018), https://home.treasury.gov/news/press-releases/sm556; Press Releases, OFAC, 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group' (2 March 2020), https://home.treasury.gov/news/press-releases/sm924.

31 id.

32 See 'Treasury Sanctions Individuals Laundering Cryptocurrency for Lazarus Group', *supra* note 30.

33 See Press Releases, OFAC, 'Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft' (16 September 2020), https://home.treasury.gov/news/press-releases/sm1123.

34 OFAC, 'Virtual Currency FAQ 559', *supra* note 32 (OFAC defines a 'digital currency address' as 'an alphanumeric identifier that represents a potential destination for a digital currency transfer. A digital currency

SDNs and other blocked persons. This new type of information, which OFAC expects to be part of standard screening protocols, typically entails a more arduous screening process due to the difficulty of searching these addresses in the SDN List.[35]

OFAC has also noted that as various sanctioned jurisdictions (e.g., Iran, Russia, North Korea) resort to using or creating digital currencies, the risk entailed in the digital currency sector may increase.[36] The mere use of certain digital currencies could be subject to blanket prohibition, which has already occurred with respect to the 'petromoneda' digital currency issued by the government of Venezuela.[37] As more government-backed digital currencies are issued, this will be an evolving risk area.

Inadvertent exports to sanctioned jurisdictions

Another potential area of compliance risk is the cybertheft of export-controlled information for use in a sanctioned jurisdiction. Any such cyber-enabled theft may represent an unauthorised and illegal export of controlled US technology or software. While such an event may raise more direct export control compliance concerns, especially depending on the nature of the stolen technology or software, OFAC could potentially consider a victim entity accountable for facilitating a sanctions violation for failing to implement appropriate risk-based measures to prevent the compromise and export of the controlled information (e.g., inadequate data security). This scenario highlights that in addition to sanctions regulations, entities should also consider other areas of related compliance risk implicated by malicious cyber-enabled activities, including export controls.

Practical considerations to mitigate cyber-related sanctions compliance risks

In response to the risks described above, and depending on the circumstances, companies may want to consider some of the following compliance measures.

Risk assessment and risk-based compliance programme

Depending on the nature of a company's business activities, the risks and challenges in complying with cyber-related sanctions may differ substantially. Conducting an appropriate risk assessment, and tailoring a risk-based compliance programme appropriately, are essential steps in mitigating risk. This is especially true in the current environment due to the global pandemic, as businesses of any size that utilise the internet, even if only for e-mail, may face an increasing risk of ransomware attacks, which raise cyber-related sanctions compliance concerns. Businesses involved in e-commerce could potentially face higher cyber-related sanctions compliance risks, including the risk of inadvertently providing goods or services to a sanctioned person or jurisdiction. Those involved in the digital currency sector, including

address is associated with a digital currency wallet'. OFAC, 'FAQ 559' (19 March 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/559.

35 See OFAC, 'Virtual Currency FAQs 562' (19 March 2018), '563' (6 June 2018) and '594' (6 June 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626.

36 See e.g., 'Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses', *supra* note 30.

37 EO No. 13,827, 83 Fed. Reg. 12,469 (19 March 2018).

companies that facilitate or engage in online commerce or process transactions using digital currencies, may be more likely to face malicious cyber-enabled attacks, incurring increased sanctions compliance risks. These risks could be even greater for companies involved in providing cyber insurance, digital forensics services, cyberattack incident response services and financial services that facilitate ransom payments.

Risk-based screening, due diligence, and IP blocking measures

Depending on a company's risk profile, it is often best to ensure that all relevant parties are properly screened before engaging in a transaction, to ensure no payments or deliveries of goods or services are made to sanctioned parties or jurisdictions. Reliable screening depends on the collection and review of information reasonably accessible to the company, which means companies should proactively consider ways to verify users' identities and locations. As evidenced in the *BitGo* settlement, merely relying on attestations from users concerning their locations without conducting any further due diligence may not suffice to meet one's compliance obligations in OFAC's view.

As the world becomes more digitised, the screening function must adapt as well. Companies should consider including a party's IP address information in the screening process when such information is available. A company may need to implement IP blocking measures to prevent sanctioned persons and persons in sanctioned jurisdictions from opening accounts on the company's website or platform that would allow them to access the company's services.

Identify, block, and report sanctioned digital currency

Companies engaged in or reliant upon digital currency have the same obligations with respect to US sanctions law compliance as they would when conducting transactions in traditional currencies. OFAC has included certain digital currency addresses associated with blocked persons as part of its set of identifiers on the SDN List, meaning that companies may have obligations to block digital currency payments associated with those digital addresses.[38] Companies that may transact routinely with such digital currency addresses should consider enhancing their screening and compliance processes to account for this information.

Screening a digital currency address is more involved than ordinary name or physical address screening, but OFAC has provided some guidance on how to search the SDN List for these addresses. OFAC guidance also provides two discrete methods companies may integrate into their compliance programme to block digital currencies held by sanctioned persons.[39] Companies may block digital wallets associated with digital addresses identified and sanctioned by OFAC, or combine all digital wallets with digital addresses identified by OFAC into one digital wallet. OFAC also requires companies holding wallets with blocked digital

38 See OFAC, 'Virtual Currency FAQs 562–63, 594', *supra* note 36. See generally OFAC, 'Virtual Currency FAQs', https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626. See also OFAC, 'Virtual Currency FAQs', https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1626 (accessed 3 May 2021).

39 See OFAC, 'Cyber-Related Sanctions FAQ 646' (28 November 2018), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546.

addresses to report the digital currency to OFAC within 10 business days and to have a traceable audit trail.

Compliance related to making or facilitating ransom payments

Given the risks associated with ransomware payments and the possibility that sanctioned persons or jurisdictions may be involved in them, sanctions compliance programmes should incorporate risk-based procedures for responding to ransomware attacks, including, at a minimum, thorough enhanced screening procedures. In many cases, companies should strongly consider engaging with relevant law enforcement agencies when ransomware attacks arise, including OFAC if the ransomware attack or a requested ransom payment may potentially involve a sanctioned party or country.

Preventative measures regarding cyber intrusions

In looking to root causes, businesses may also reduce their cyber-related sanctions compliance risks by making efforts to prevent cyber intrusions in the first place. US government agencies, including the US Department of Treasury Financial Crimes Enforcement Network[40] and the US Department of Justice,[41] have provided guidance on best practices for companies to help them protect their systems from such cyberattacks. Integrating these considerations into a company's overall approach to risk management and, specifically, its sanctions compliance programme in the first instance can prevent sanctions violations arising from malicious cyber-enabled activities (e.g., ransomware attacks) carried out by a sanctioned party or country.

Potential benefits of cooperation with the US government in the cybersecurity context

We close by highlighting the strong incentives that US government enforcers provide in exchange for voluntary disclosure and robust cooperation by companies that have committed potential US sanctions violations, which apply equally in the cyber context. For example, in the OFAC ransomware advisory discussed above, OFAC emphasised that it would consider both a 'self-initiated, timely, and complete report of a ransomware attack to law enforcement' and 'full and timely cooperation with law enforcement' to be 'significant' mitigating factors in determining the proper enforcement outcome if a ransom payment is made and 'if the situation is later determined to have a sanctions nexus'.[42] Likewise, in the SAP enforcement matter discussed above, the Department of Justice explained that SAP's penalty 'would have been far worse had they not disclosed, cooperated, and remediated. We hope that other businesses, software or otherwise, we heed this lesson.'[43] OFAC also touted SAP's 'substantial'

40 FinCEN, 'Advisory on Illicit Activity Involving Convertible Virtual Currency' (9 May 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf.

41 US Dep't of Justice et al, 'How to Protect Your Networks from Ransomware: Interagency Technical Guidance Document' (June 2016), https://www.justice.gov/criminal-ccips/file/872771/download.

42 OFAC, *supra* note 18, at 4.

43 Department of Justice, SAP Admits to Thousands of Illegal Exports of its Software Products to Iran and Enters into Non-Prosecution Agreement with DOJ (29 April 2021), https://www.justice.gov/opa/pr/sap-admits-thousands-illegal-exports-its-software-products-iran-and-enters-non-prosecution.

cooperation and significant remedial actions, as well as its voluntary disclosure, in explaining why the actual penalty was reduced substantially from the civil penalty recommended under OFAC's enforcement guidelines. Although cooperation with US government enforcers is a complex, risk-based decision that must be considered carefully, the potential benefits are clear under the right circumstances.

Appendix 2

About the Authors

Brian Fleming
Miller & Chevalier Chartered

Brian Fleming, member at Miller and Chevalier, focuses his practice on investigations and compliance counselling in matters at the intersection of international trade and national security with an emphasis on economic sanctions, export controls and foreign direct investment. Mr Fleming advises leading US and foreign companies on compliance issues implicating the Treasury Department's Office of Foreign Assets Control, the Commerce Department's Bureau of Industry and Security and the State Department's Directorate of Defense Trade Controls. He conducts internal investigations, coordinates responses to subpoenas and other investigative demands and represents companies and individuals in government enforcement actions.

Mr Fleming counsels US and foreign companies with respect to the Committee on Foreign Investment in the United States (CFIUS) process from pre-transaction risk assessments to preparation of voluntary and mandatory CFIUS filings and management of mitigation agreements. Additionally, Mr Fleming concentrates on core national security issues and advises clients on matters relating to cybersecurity, the Foreign Agents Registration Act, Foreign Ownership, Control, or Influence, the Foreign Intelligence Surveillance Act and Department of Justice investigations of media leaks and disclosures of classified information. Mr Fleming also hosts the firm's economic sanctions and export controls podcast, EMBARGOED!

Timothy O'Toole
Miller & Chevalier Chartered

Timothy P O'Toole is the leader of Miller and Chevalier's white collar defence practice group. Mr O'Toole focuses his practice on defending enforcement actions and conducting investigations involving the economic sanctions, export controls and anti-money laundering laws. Recognised as one of the leading international trade lawyers in the US by *Chambers USA*, *The Legal 500*, *Who's Who Legal*, and *Global Investigations Review*, Mr O'Toole provides companies

and individuals with advice on compliance with the US economic sanctions, export controls and anti-money laundering laws, and interacts regularly with US Department of Justice, the Treasury Department's Office of Foreign Asset Control, the State department's Directorate of Defense Trade Controls and the Commerce Department's Bureau of Industry and Security in that capacity.

Mr O'Toole writes and speaks often about white collar defence and international trade issues globally at venues and media outlets. He is a past co-chair of the National Association of Criminal Defense Lawyers (NACDL) West Coast White Collar Crime Conference in Santa Monica and a past co-chair of the NACDL's White Collar Crime Committee. Mr O'Toole also hosts the firm's economic sanctions and export controls podcast, EMBARGOED!

Caroline Watson
Miller & Chevalier Chartered

Caroline Watson is a senior associate in the international department. She focuses her practice on international trade, with emphasis on export and import controls, economic sanctions and customs.

Growing up in the Middle and Far East and traveling extensively around the world, Ms Watson brings a keen understanding of international issues and cross-cultural communication to serve clients in international trade-related matters. She counsels clients concerning issues related to imports and exports (including International Traffic in Arms Regulations and Export Administration Regulations), the Foreign Corrupt Practices Act, customs, free-trade zones, economic sanctions, and defence article operations. Ms Watson has experience developing compliance programmes, conducting internal investigations and regulatory compliance audits and representing clients in government inspections and investigations. She also advocates clients' interests regarding compliance issues in submissions to and conferences with various government agencies, including the Directorate of Defense Trade Controls, the Office of Foreign Assets Control, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the Alcohol and Tobacco Tax and Trade Bureau, the Bureau of Industry and Security, US Customs and Border Protection and the US Department of Justice.

Manuel Levitt
Miller & Chevalier Chartered

Manuel (Manny) Levitt is an associate in Miller and Chevalier's international department. He focuses his practice on economic sanctions and export controls.

Prior to joining the firm, Mr Levitt gained experience in international trade at an Am Law 100 firm, where he helped global businesses address a wide variety of legal and regulatory challenges affecting their cross-border supply chains, transactions and operations. He has advised clients on matters related to regulations administered by the US Customs and Border Protection, the Treasury Department's Office of Foreign Assets Control, the Commerce Department's Bureau of Industry and Security and the State Department's Directorate of Defense Trade Controls. He also has experience helping clients comply with anti-corruption and anti-forced labour laws, assisting with internal investigations, and representing clients before federal agencies.

Mr Levitt graduated with honors from The George Washington University Law School, where he was a member of the *Public Contracts Law Journal* and the Anti-Corruption and Compliance Association. He was awarded a Foreign Language and Areas Studies Fellowship, during which he studied Mandarin Chinese and took courses on Chinese legal institutions and Chinese business law.

Mary Mikhaeel
Miller & Chevalier Chartered

Mary Mikhaeel is an associate in Miller and Chevalier's international department. She focuses her practice on international trade matters, including economic sanctions, export compliance, import compliance and trade policy. Ms Mikhaeel advises clients on issues related to the US Department of the Treasury's Office of Foreign Assets Control, US Department of Commerce's (DOC) Bureau of Industry and Security and US Customs and Border Protection. She has experience in developing compliance programmes, conducting internal investigations and assisting clients with ruling requests.

Prior to joining the firm, Ms Mikhaeel worked at another DC law firm where she focused her practice on international trade and government contracts matters. Ms Mikhaeel was a law clerk for the DOC's Office of the Inspector General and an intern for the DOC's International Trade Administration, Commercial Service.

While attending law school, Ms Mikhaeel was president of the International Law Society and was dedicated to helping law students learn more about international law and meet practitioners in DC. She was an associate on *The George Washington International Law Review.*

Miller & Chevalier Chartered
900 16th Street NW
Black Lives Matter Plaza
Washington, DC 20006
Tel: +1 202 626 5800
bfleming@milchev.com
totoole@milchev.com
cwatson@milchev.com
mlevitt@milchev.com
mmikhaeel@milchev.com
www.millerchevalier.com

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

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

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

an LBR business

ISBN 978-1-83862-596-2