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

21

The Role of Forensics in Sanctions Investigations

Amy Njaa, A. Walid Osmanzoi, Nicholas Galbraith and Adetayo Osuntogun[1]

Introduction

The global value chain is a far-reaching system reliant on cross-border transfers of funds, services and goods, which are increasingly subject to economic sanctions and export controls law enforcement by the Office of Foreign Assets Control (OFAC), the US Department of Justice (DOJ) and other authorities. Investigations involving sanctions allegations will continue to be more prevalent as sanctions are a growing foreign and security policy tool used to influence foreign behaviour and mitigate national security risks.

Parties seeking to circumvent the sanctions regulations often go to great lengths to disguise transactions using intricate payment processes, subsidiaries, intermediaries and shell corporations, among other vehicles. To combat these types of deception, organisations should implement effective sanctions compliance programmes and investigate potential sanctions violations. Thus, prudent companies will leverage cutting-edge investigative techniques, tools and consultants with specialised forensic knowledge. The purpose of this chapter is to explain key investigative procedures and best practices from a forensic accounting perspective and highlight the techniques and tools used to uncover facts and patterns in the complex web of sanctions-related transactions. The chapter provides a combination of best practices, published guidance from OFAC and recent case outcomes to provide insight on the evolving sanctions environment and to support forensic and compliance professionals in creating, enhancing or testing an existing sanctions compliance programme (SCP).

---

1 Amy Njaa is a director and A. Walid Osmanzoi is a manager, at BDO USA LLP, and Nicholas Galbraith and Adetayo Osuntogun are associates at Barnes & Thornburg LLP. The authors would like to acknowledge the contributions of Linda Weinberg and Roscoe Howard of Barnes & Thornburg LLP and Nicole Sliger and Pei Li Wong of BDO USA LLP.

OFAC guidance

OFAC's guidance document, 'A Framework for OFAC Compliance Commitments', encourages companies to 'develop, implement and routinely update' a risk-based SCP.[2] OFAC strongly recommends the adoption of an SCP by all organisations subject to US jurisdiction and foreign entities that conduct business in or with the US or US persons, or that use US origin goods or services, use the US financial system, or process payments to or through US financial institutions. Forensic methodologies and tools are critical elements of compliance measures such as risk assessments and compliance testing. For the purposes of this chapter, we focus on the two SCP components most relevant to forensics – risk assessment and testing or auditing – and how these components interplay with the factors OFAC considers in administrative enforcement actions.[3]

The risk assessment and testing and auditing components of an SCP should not be viewed in isolation, but rather should inform each other and continue to evolve. Not only is the regulatory environment constantly evolving, so too is the nature of a business. Because each company is unique, the risk assessment, and testing and auditing plan should be tailored to each business. Additionally, risk assessments should be refreshed periodically. A proper risk assessment and testing and auditing cycle should minimise exposure in the event of an apparent violation. Moreover, the conclusions should be analysed as part of the testing and auditing process. If testing or auditing reveal that risks are higher than anticipated in one portion of the business, these results should inform the company's risk assessment and compliance efforts.

As OFAC notes, a risk assessment should consider customers, products, services, supply chain, intermediaries, counterparties, transactions and geographical locations, depending on the nature, size and sophistication of the organisation. These factors should be targeted for assessment during the testing and auditing process. When determining the appropriate administrative action in response to a sanction violation, OFAC will follow and consider certain 'general factors' described in its Economic Sanctions Enforcement Guidelines.[4]

Implementing a testing and auditing plan as part of a risk-based SCP is a mitigating factor. However, using key forensic procedures and analytical tools as part of a testing and auditing plan can also help reduce a company's exposure by minimising instances of aggravating conduct. For example, auditing using forensic procedures and data analytical tools on emails and shipping records can help detect and deter knowing non-compliance by employees.

---

2 See https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

3 A Framework for OFAC Compliance Commitments states: 'OFAC has generally focused its enforcement investigations on persons who have engaged in wilful or reckless conduct, attempted to conceal their activity (e.g., by stripping or manipulating payment messages, or making false representations to their non-US or US financial institution), engaged in a pattern or practice of conduct for several months or years, ignored or failed to consider numerous warning signs that the conduct was prohibited, involved actual knowledge or involvement by the organization's management, caused significant harm to US sanctions program objectives, and were large or sophisticated organizations.'

4 31 CFR Part 501, Appendix A, at www.ecfr.gov/cgi-bin/text-idx?SID=12391671113187bb461c66f657262bff&mc=true&node=ap31.3.501_1901.a&rgn=div9.

Key forensic procedures and analytical tools

Data analysis

Among the most effective investigative procedures applied in testing or investigating an SCP is a statistical analysis of historical and 'real-time' transactional data. It is critical that a company can identify potentially suspicious transactions and determine the 'who, what, where, when and how' by piecing together a timeline of events.

Statistical data analysis, ranging from basic pivot-table analysis to more advanced software applications and platforms to stratify, synthesise and flag data from a variety of ecosystems, is an invaluable tool. The key to effectively using data analysis is the ability to link transactional evidence buried in a multitude of data fields from disparate sources to identify hidden relationships or correlations.

With the assistance of data analytic tools, robust forensic analysis can be performed to help thwart sanctions violations. The following observations from recent enforcement cases (as discussed in more detail in the section that follows) could further assist in preventing and detecting potentially suspicious activities:

- *Identify third parties at high risk for sanctioned country activities and use software or data analysis (or both) to block or monitor transactions with those parties.* For example, sales to global trading companies present elevated risk because there is often no transparency regarding the end user of a product sold to them. An organisation should perform its own risk-based due diligence on third parties and consider using software programmes (e.g., IP address blocking software) or data analysis to block or monitor transactions for 'red flags'.
- *Incorporate neighbouring sanctioned country activity in data analysis, including monitoring bills of lading and other commercial documents for ports of unlading.* Shipping documents indicating a destination in a country neighbouring a sanctioned country – particularly Iran – may raise concerns about illegal trans-shipment. Data analysis can flag these transactions for further review. Transactions involving countries with robust global trans-shipping, such as the United Arab Emirates, should be closely scrutinised in respect of sensitivity to risk.
- *Use keyword searches on unstructured data to assist with data analysis.* Evidence regarding prohibited transactions is frequently located in unstructured data (e.g., electronic communications such as email, voicemail and instant messages). Forensic tools can identify suspicious activity using keywords on these communications, including metadata reviews (e.g., to/from fields). Further, a company can proactively use keyword searches across communication channels in the normal course of business to identify suspect transactions or 'code' words or phrases in real time and to block those communications.
- *Consider local practices, processes and procedures for data storage and tracking, external integrated systems (e.g., on local computer drives).* Businesses in many countries often use 'offline' spreadsheets to track transactions. While it is important to analyse data from integrated company systems, one must also consider transactions recorded or tracked 'off the books'. US parent companies of foreign subsidiaries with a history of, or at elevated risk for, sanctioned country transactions should consider remote monitoring of local computer drives and servers and use of mirrored drives in periodic audits. Local privacy laws must also be taken into consideration.

- *Employ an automated project proposal management system to automatically flag and block questionable projects for further review.* US parent companies should have access to this system and routinely monitor it to prevent foreign subsidiaries from engaging in prohibited transactions with parties in sanctioned countries.
- *Automate travel expense process and screening.* Travel expense reports can provide insight on work location. An automated travel expense report system, which screens destinations, can help detect services to sanctioned countries or denied persons. Filtering data fields and searching for unusual keywords in travel expense systems, such as 'vacation' (which may be an obfuscation of a business trip to a sanctioned country), can identify discrepancies in client name, address, mileage, currency, among other things. To illustrate, a travel expense report indicating travel to Armenia with receipts showing currency in Iranian rial (the local currency) could be flagged with data analysis. Travel expenses should be audited frequently.
- *Monitor service contracts and warranties.* Companies should consider accumulating service contracts and warranties in a system or database to identify and block service transactions involving prohibited business in sanctioned countries. Companies should also consider using data analysis to identify discrepancies between service contracts or warranties and related documents (e.g., payment or travel records) and to flag potentially high-risk service contracts or warranties with countries that are near sanctioned countries.

Investigative due diligence

Investigative due diligence typically comprises a set of research tools and approaches that can be applied to a wide range of investigations. In sanctions-related investigations, these tools may consist of (1) documents and electronic records disclosed by a party, (2) public records gathered through desktop research or on-site searches, and (3) observational site inspections or human source intelligence. Investigative due diligence arms investigators with additional knowledge to connect dots and enhance understanding of the pool of information gathered about the subject of the investigation.

Additionally, forensic professionals leverage investigative due diligence to combine data analysis with a review of pertinent open-source data about the parties involved in the activity. Open-source data (e.g., public records such as corporate registry details, litigation records, asset ownership details and social media) can assist with untangling the web of indirect relationships and interrelated connections involved in transactions. Although the investigative trail often begins with the company's books and records, perpetrators usually engage in a variety of techniques to cover their tracks, such as layering and multiple transfers to intermediaries, shell companies, nominee shareholders and related parties. By using investigative due diligence, including reviews of public records and 'boots on the ground' interviews, investigators can uncover valuable clues regarding ownership structure and executive leadership positions of complex organisational structures.

Perpetrators may go to significant lengths to obscure beneficial ownership of companies or to disguise certain transactions, but these patterns can often be identified with common elements such as addresses, proxies or nominees in corporate structures, or law firms or accountants used to register companies. Investigators frequently use link analysis and other visualisation tools to track the information uncovered, map the networks of bad actors, and help companies understand the potential exposure to those bad actors. Identifying patterns

or connections in voluminous information requires tools to distil the information quickly and clearly into charts or graphs.

Supply chain mapping

Forensic analysis tools also enable the use of models for predictive analysis and present opportunities for global supply chain mapping. This mapping offers the possibility to identify the sanctions risk posed by third parties such as suppliers, distributors, agents, sub-agents and customers who may be doing business directly or indirectly with sanctioned countries, or whose activities benefit sanctioned governments or sanctioned persons.

When supply chains extend to countries that actively trade with sanctioned jurisdictions, the sanctions risk may be elevated. Some primary examples of these relationships include Colombia and Venezuela, China and North Korea, United Arab Emirates and Iran, Iraq and Syria, and Russia and North Korea. Assessing the potential third-party risk of relationships should be a process in which data analysis and models are continually updated with new information taken from the latest enforcement actions, in addition to published advisories from the US State Department, US Treasury Department or other authorities.

Investing in developing a supply chain risk map will produce longer-term benefits, especially for larger, complex enterprises and those with a multinational presence. The insight gained through supply chain mapping for sanctions risk will help in designing effective internal controls, training programmes and due diligence practices.

Predictive analysis

Once a supply chain is mapped for sanctions risk, predictive modelling can be leveraged with a global SCP to identify emerging trends in the evolving global sanctions landscape. For example, enterprises that deliver fourth-party or fifth-party logistics services[5] can enhance their existing contingency plans by incorporating sanctions risks in their supply chain mapping. Predictive analysis can highlight counterparties and relationships that may need to be re-evaluated or replaced in the event of a sanctions-related disruption, such as a sanctions designation or significant enforcement action. Although not widely adopted, there is a growing number of companies who are using predictive analytics.

Leveraging key forensic procedures and analytical tools such as those described above will assist in building a 'best-in-class' SCP. Due to exponential growth of international transactions, reliance on manual compliance controls alone can no longer effectively protect organisations against costly enforcement actions or other risks.

On-site interviews and inspections

Forensic investigations rely heavily on historical records to identify relevant facts and support conclusions. Interviews or on-site observations provide additional context on collected data or evidence to validate authenticity and confirm facts and circumstances leading up to the recording of transactions. Live observation of body language can also be very valuable,

5 In using fourth- and fifth-party logistics service providers, companies outsource a majority of, or nearly all, logistics management activities. As more of the supply chain logistics function is performed by an external party rather than the company itself, compliance risk increases.

especially in potentially sensitive situations involving possible wrongdoing. For this reason, on-site interviews or inspections present unique opportunities for compliance personnel, investigators or those engaged to perform related testing.

In practice, live interviews can help investigators evaluate employees' compliance policy knowledge and the effectiveness of training, which may shed light on documented decisions made by those employees. This can potentially distinguish intentional violations of policy from decisions made because of deficient training or human error. These 'live' meetings provide first-hand knowledge of how written policies and procedures are operating. In some cases, disparities between the written procedure and its execution might point to gaps in the procedure. Process walk-throughs can also detect procedural steps skipped by employees taking 'shortcuts'. Interviewees can articulate why certain procedures were not performed and describe pain points or process inefficiencies that exist, highlighting the need for policy updates or additional controls.

Field interviews and observations can also detect instances when compliance processes are viewed as unimportant by employees or management, or are not adequately supported by funding, necessary equipment, information technology infrastructure or staffing. These observations may indicate an overall lack of management commitment to the programme or a failure to anticipate external stresses. For example, employees in economically developing countries, where disruptions to internet service (or even electrical power) are commonplace, may default to unapproved work arounds or off-system processes, which result in incomplete system data and failures to apply controls.

Irrespective of geography, protracted crisis may result in lengthy business interruption, high staff turnover or absenteeism. Employees may be unable to access their work location because of civil unrest, natural disaster or other widespread disruption, as exemplified by the covid-19 pandemic that began in 2020 and the Myanmar military coup that occurred in 2021. Thus, expertise or resources required to fully execute the SCP may not be available and employees may find themselves under increased pressure to ignore processes for the sake of business continuity. Sanctions compliance should influence the crisis response and business continuity plans for sophisticated, global organisations. Advance planning and on-site walk-throughs help to provide a clearer picture in understanding potential risks, which may not be anticipated or detected during a crisis.

In situations where on-site procedures cannot be performed, such as the travel constraints brought on by the covid-19 pandemic, interviews and inspections conducted remotely can provide satisfactory results when investigators adhere to best practices. Video conferencing allows the interviewer to gauge the interviewee's body language and facial expression, may help to put the interviewee at ease and can provide a solution for remote sharing of documents on a shared screen. The use of mobile devices to allow a view of facilities can be effective when an in-person inspection is not possible. However, investigators also need to be aware of pitfalls when conducting remote procedures. A keen awareness of relevant data protection or privacy laws and regulations, state and commercial secret laws and employment regulations is key to successful remote interviews and inspections.

Data preservation and collection activities are major activities in an investigation. Forensic practitioners collect data from servers and devices such as smartphones, laptop computers, hard drives and other portable drives (e.g., flash drives). While remote collection of server data is a common industry practice, collecting data from other devices in a forensically sound

way may require shipping of such devices and is often challenging and slow, especially in times when global logistics services are overextended due to the covid-19 pandemic.

Many organisations still rely heavily on hard copy documentation to conduct business. Often, the need to maintain hard copy paper trail is frequently driven by local government requirements and business norms in the country. Organisations may scan hard copy documents for electronic storage, but the quality of the scan is often inconsistent and scanned images are at risk of being altered. Best practice is to follow up with an onsite examination of the original hard-copy documentation when able.

For remote interviews, interviewers should be alert to the possibility of other individuals in the same room who may be coaching the interviewee or listening in. An interviewee may try to avoid being interviewed or answering questions by claiming technical difficulties. Remote interviews also run the risk of being recorded surreptitiously. During virtual tours of facilities and premises, investigators should expect areas of interest to the team may be intentionally excluded from the tour. If permissible, investigators can arrange to have local colleagues be present in person during remote procedures to mitigate these risks.

One major limitation of remote procedures is the inability to conduct unscheduled interviews or surprise 'spot checks'. These cannot be performed remotely, mainly because of the coordination and logistics arrangements required to organise remote data collection, interviews or facilities inspections.

Ultimately, proper planning is key, and communication of expectations to the subject entity or individual help reduce misunderstanding over logistics. Where possible, the investigations team should corroborate preliminary results from the remote investigative procedures by supplementing the work conducted with an in-person inspection when travel becomes feasible.

Potential post-investigation procedures

An investigation should conclude with a final report containing findings. An opportunity exists to convert findings into formalised action plans to remediate deficiencies. For example, when gaps in compliance knowledge are revealed, the organisation should implement role-specific or targeted training. A finding that screening systems failed to detect name variations may result in new rules within the screening system. Still other findings may require enterprise-wide initiatives and policy development.

Specific compliance errors uncovered through transaction analysis and forensic techniques, such as look-backs, are also useful to isolate incorrect compliance decisions and enhance existing training programmes and materials. The circumstances surrounding the errors are useful in forming situation-based questions and case studies for training materials, discussions and employee examinations. Studying the various types of errors may also be helpful in creating automated system-generated policy reminders to help employees in following the correct steps to avoid a violation.

Action plans should include: responsible parties, follow-up timelines, and procedures with features such as scheduled action plan updates; re-training or re-testing of employees; follow-up sampling of transaction activity to test controls; updated or enhanced risk-assessments; targeted disciplinary actions such as probationary periods or re-evaluation of contracts with external parties. Follow-up activities associated with an action plan should also be documented and records retained according to written policy and legal standards.

Analysis of recent enforcement cases – a forensics focus

Examining recent cases and outcomes offer insight into trends within the evolving sanctions landscape. This context is important to demonstrate the application of various forensic investigative methods and best practices, while also highlighting the practices that might have contributed towards the identification of mitigating factors considered by OFAC.

BitPay, Inc.

This 2021 action[6] highlights the importance of online businesses having an effective internet protocol (IP) address-blocking strategy. BitPay, Inc. (BitPay) is a company that offers a payment processing solution using digital currency as payment for goods and services. BitPay receives digital currency payments on behalf of its merchant customers from those merchants' buyers, converts the digital currency to official currency, and then relays that currency to its merchants. BitPay screened its direct customers, who were the merchants, against OFAC's Specially Designated Nationals and Blocked Persons (SDN) List. However, BitPay's transaction review process did not fully analyse location data that it sometimes obtained about its merchants' buyers, including name, address, email address, phone number and IP address. As a result, buyers with indicators showing they were located in Crimea, Cuba, North Korea, Iran, Sudan and Syria were able to make purchases on BitPay's platform.

BitPay may have benefited from more systematic collection and mining of buyer data at the time of the transaction, including deployment of an IP address-blocking software. Software that would automatically block the creation of invoices listing the buyer's address in an embargoed country would also help prevent violations. Forensic tools, such as geolocation analytics on IP/MAC addresses, can also be used to periodically identify transactions for embargoed countries.

Berkshire Hathaway Inc.

This 2020 action[7] showcases the risks for US-based parents of foreign subsidiaries. Berkshire Hathaway Inc. (Berkshire), a US company, has a Netherlands-based subsidiary, IMC International Metalworking Companies BV (IMC), which in turn has a Turkish subsidiary. The Iran sanctions programme prohibitions extend to knowing activities by non-US entities owned or controlled by US persons, such as Berkshire, and the US parent can be penalised for the activities of their foreign subsidiaries. According to OFAC, the Turkish IMC subsidiary knowingly engaged in transactions with persons subject to the jurisdiction of Iran, including by selling items to Turkish intermediaries with knowledge that the items would be supplied to an Iranian distributor for resale to Iranian end-users. The Turkish IMC subsidiary apparently took steps to hide its Iranian transactions from other Berkshire subsidiaries by using cash payments, false invoices and communications through private, non-business email. Nonetheless, in OFAC's view, other IMC subsidiaries had access to information indicative of the Iranian connection, including email chains containing an address indicating that the distributor was in Iran and email chains referencing a customer known to a subsidiary located in Iran.

6 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210218.

7 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201020.

Berkshire may have been able to identify such prohibited activity through periodic reviews of emails and instant messages using key word searches. Employee interviews, email metadata reviews (e.g., to and from addresses) and employee portals for anonymous whistle-blowing may also raise red flags.

Société Internationale de Télécommunications Aéronautiques SCRL

This 2020 case[8] demonstrates risks posed to providers of software services, especially when those services are routed through or hosted on servers located in the United States. Société Internationale de Télécommunications Aéronautiques SCRL (SITA), an organisation with membership open to aviation operators worldwide, provides software services for the aviation industry. OFAC investigated SITA after discovering three members were Iranian and Syrian airlines named as specially designated global terrorists (SDGTs). At the time OFAC designated these airlines as SDGTs, SITA reviewed its agreements with the airlines and terminated their access to ticketing, airfare, e-commerce and other services. However, SITA continued to provide certain messaging, check-in and baggage tracking services that benefited the SDGT airlines directly or indirectly. These services were routed through the United States, maintained on servers located in the United States or performed using a software application with US origins. OFAC deemed the provision of those services to be a violation of the Global Terrorism Sanctions Regulations.

SITA may have benefited from a more thorough review of its services and software, not just a manual review of the agreements with these Iranian airlines. For example, software and services provided to SITA's member airlines and other third parties could indirectly benefit the SDGT airlines, depending on their commercial relationships. Comprehensive testing of usage for all software and services may have identified the ultimate beneficiaries of these products. For example, forensic analysis could include an examination of the software, the software support servers and their functionalities, and more importantly, written policies and procedures regarding software-to-server communications from sanctioned locations and obfuscated IP addresses, which may have revealed where the SDGTs had received or accessed the software.

Apollo Aviation Group, LLC

This 2019 case[9] demonstrates the need to track the end-use of assets leased to third parties. Apollo Aviation Group, LLC (Apollo) leased three aircraft engines to an airline, which subleased the engines to a sub-lessee that installed them on aircraft leased to a Sudanese SDN. Apollo's lease contained a sanctions compliance provision, but OFAC noted that Apollo failed to monitor or otherwise verify the actual whereabouts of its engines during the lease term.

Effective methods for monitoring and tracking assets will vary by industry and asset type, but companies should consider the following:

- obtaining export compliance certificates from both lessees and sub-lessees;
- including lease provisions that allow the lessor to verify location of its assets and conduct end-use audits;

8 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200226_33.

9 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20191107_33.

- requiring lessees to provide information on asset users and location, and the procedures used to make that determination;
- monitoring asset location and use via access logs and geographical location logs, as tracked by embedded software; and
- requiring the lessee to track the location of its assets using barcode scanning and making the system accessible to the lessor.

The General Electric Company

This 2019 case[10] highlights the importance of employing screening best practices and 'know your customer' due diligence. The General Electric Company (GE) accepted payment from a third party on behalf of a Canadian customer of GE. The third party, a Cuban SDN, was an entity owned by a public joint venture between the Canadian customer and the Cuban government. The third party's cheques showed its full legal name and an acronym, but GE only screened the acronym and did not flag the SDN. GE also failed to flag its Canadian customer's ties to the Cuban SDN, despite a long-term customer relationship that had been renewed on multiple occasions.

The lessons learned include that companies should (1) verify that the screening software incorporates fuzzy logic and common name variations for SDNs, such as acronyms, (2) train employees to screen known variations of a party's name, and (3) periodically review – or engage a service provider to review – publicly available information about their customers' business for sanctions-related red flags. Regularly monitoring business partners to understand interrelated parties and uncover possible indications of sanctioned country business can help to prevent inadvertent violations.

Kollmorgen Corporation

In this 2019 settlement,[11] Kollmorgen, a US company, acquired a Turkish company (the 'subsidiary'). Kollmorgen performed due diligence prior to closing and discovered that the subsidiary made sales to Iran. The subsidiary continued to provide services and products to Iran for two years post-closing by employing fraudulent techniques, including falsifying travel reports, deleting and falsifying emails and other records, and providing false compliance certifications. Kollmorgen ultimately discovered the violations through an ethics hotline call from an employee of the subsidiary.

As stated by OFAC, this case highlights the importance of (1) performing heightened due diligence on affiliates, subsidiaries or counterparties known to have transacted with OFAC-sanctioned countries or persons, or that otherwise pose a high risk owing to their geographical location, customers, distributors or suppliers, or products and services, and (2) implementing proactive controls when US persons acquire interests in companies with existing sanctioned country or SDN relationships. Because services can be more difficult to track than products, additional scrutiny of service providers is warranted. Additionally, as noted above, data analysis using keywords in travel expense systems (e.g., vacation or personal) may have allowed the parent company to identify suspicious travel to Iran in real time.

10 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20191001.

11 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20190207.

A closer look at supply chain issues

Recent OFAC actions highlight specific supply chain issues that can also be addressed using various forensic investigative methods.

Xinjiang Supply Chain Business Advisory

This July 2020 multi-agency advisory[12] sounds an alarm on supply chain risks associated with forced labour and other human rights abuses in the Xinjiang region of China. The Advisory identifies potential indicators of forced labour and labour abuses, such as:

- lack of transparency (e.g., use of shell companies to obscure the source of goods);
- lack of employees paying into social insurance programmes;
- the company's receipt of government development assistance;
- nonstandard hiring practices or use of government recruiters;
- proximity to internment camps or adjacent to industrial parks involved in poverty alleviation efforts; and
- use of certain internment terminology such as Education Training Centres or Legal Education Centres, ethnic minority graduates, or involvement in reskilling.

Evidence of these indicators can be monitored from a forensics perspective through in-person site inspections, key employee interviews, key word searches in structured and unstructured data and regular investigative due diligence procedures.

e.l.f. Cosmetics, Inc

This January 2019 case[13] illustrates the dangers of failing to perform proper supply chain due diligence. SCP and supplier audits at e.l.f. Cosmetics, Inc (Elf) failed to uncover that approximately 80 per cent of the false eyelash kits procured from China-based suppliers contained North Korean materials. Elf's remediation measures stand out from a forensics and data analysis viewpoint: (1) implementing supply chain audits that verify the country of origin of goods and services used in its products; and (2) conducting enhanced supplier audits that include verification of payment documentation for materials and review of supplier bank statements (access to a supplier's records is best negotiated with the supplier as a condition of receiving payment). In addition, purchasers should consider performing data analytics on product components or ingredients (e.g., researching the sources of the product or its major constituent materials to determine whether sanctioned countries are significant manufacturers and, if so, whether they are located near the supplier country). As described in detail above, third-party risk assessment, supply chain due diligence and supply chain mapping assist in identifying potential red flags for sanctions-related issues.

Sanctions compliance: best practices and lessons learned

Former US Deputy Attorney General Paul McNulty issued a warning at a 2009 conference that has become a popular maxim within compliance circles even more than a decade later:

12 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200701.

13 https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20190131.

'If you think compliance is expensive, try non-compliance.'[14] Sanctions compliance violations are among the costliest ways this lesson is learned. OFAC maintains the most active and extensive sanctions programme in the world. OFAC's recent output has included a steady flow of new regulations, guidelines and enhanced reporting requirements for rejected transactions.

It is worthwhile to remember that OFAC considers 'good faith' compliance efforts in the disposition of enforcement matters. OFAC 'will consider favourably subject persons that had effective SCPs at the time of an apparent violation'.[15] However, there is no way to predict how OFAC will apply this principle to individual cases, so compliance professionals and organisational leaders should not assume their efforts will result in mitigation of penalties. Take, for example, the SITA settlement, which resulted in a significant financial penalty even though SITA had taken steps to comply with the Global Terrorism Sanctions Regulations in terminating some services offered to the SDGT airlines.

The advice supplied by OFAC in the 'Framework for OFAC Compliance Commitments', and echoed here, can be traced to cases in which at least one of the five commitment areas was deficient. Focusing on the forensic and investigatory lessons that can be gleaned from the cases referenced herein, below is a series of emphatic do's and don'ts, from a forensics perspective, for building an SCP, testing an existing programme or conducting sanctions investigations.

Do…

Sanctions compliance programme

- Conduct comprehensive risk assessments.
- Implement risk-based, straightforward policies, procedures and internal controls relevant to day-to-day operations and sanction concerns.
- Enforce policies and procedures, and identify, document and remediate weaknesses.

Due diligence and screening

- Conduct diligence on customers, distributors, suppliers, contractors, logistics providers, financial institutions and other partners.
- Continuously use and test automated screening software being cognisant of filter faults – prioritise alerts by severity.
- Utilise systems to track movement of goods and financial transactions from manufacturing to end user.
- Deploy blockchain and distributed ledger technologies to improve due diligence records.
- Understand circumvention risk.
- Monitor recent enforcement actions for effects on operations.
- Establish anonymous reporting channels for employees and policies to ensure non-retaliation.

Testing and auditing

- Assess tools, technology and data needed to monitor sanctions compliance.
- Consider artificial intelligence to detect red flags – calibrate and test routinely.

14 Rodney T Stamler, Hans J Marschdorf, Mario Possamai, *Fraud Prevention and Detection: Warning Signs and the Red Flag System* (Boca Raton, FL CRC Press, 12 March 2014), page 4.

15 See www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf.

- Apply forensic investigative techniques on structured and unstructured data and metadata.
- Conduct regular internal compliance audits, including at crucial junctures, for example, mergers, acquisitions and management changes.
- Conduct supply chain audits with country-of-origin verification.
- Perform supplier and distributor audits.

Don't…

- conceal violations;
- facilitate transactions by non-US persons (including through or by non-US subsidiaries or countries);
- utilise US financial systems or process payments to or through US financial institutions for transactions involving sanctioned persons or countries (including US dollar payments); or
- utilise non-standard payments and commercial practices.

Conclusion

The area of sanctions compliance continues to grow in importance and simultaneously challenge the programmes, tools and talents of legal, compliance and forensics professionals. As the international political trends and criminal activities driving the use of sanctions show no signs of disappearing, and worldwide economic instability continues to show vulnerabilities in the global value chain, the advantage of establishing a robust and proactive SCP will provide a significant measure of protection against potential violations. By focusing on the core commitment areas described in the OFAC guidance, drawing from best practices and tools used by forensics professionals, and studying relevant case outcomes, enterprises seeking to mitigate sanctions risk can do so with confidence that those efforts will pay off in the long term.

Appendix 2

About the Authors

Amy Njaa
BDO USA LLP

Amy Njaa is a director in BDO's Minneapolis office and has over 20 years of experience in providing auditing, accounting and forensic services to private and publicly traded businesses. Over her career she has been involved in many high-profile audits, fraud investigations, litigation disputes and monitorships. Her passion lies in providing monitoring and oversight services to companies required to comply with settlement terms and corporate compliance programmes. Amy has a deep knowledge of accounting and extensive experience in evaluating internal controls, understanding complex agreements, investigating fraud allegations and addressing technical accounting and financial reporting issues.

Amy is currently a team member assisting the special compliance coordinator appointed by the US Department of Commerce to coordinate, monitor, assess and report on the US export control compliance of Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd. Prior to that, she served as a lead project manager assisting the monitor of the historic National Mortgage Settlement in evaluating one of several large financial institutions' compliance with new mortgage servicing rules and other settlement terms.

A. Walid Osmanzoi
BDO USA LLP

A. Walid Osmanzoi is a manager in BDO's Washington, DC office with over 10 years of experience in advising clients in litigation disputes, fraud investigations, investigative analytics matters, and global compliance matters in various industries. Walid has led and been involved in several high-profile RMBS securities litigation matters, monitorships and investigations of fraud perpetrated by employees, customers, and vendors. He specialises in using innovative analytical techniques and leveraging the latest technologies to identify risks and threats to an organisation's business, detect patterns and indicia of fraud, waste and abuse

in structured and unstructured data, and deliver engagements in an efficient manner bringing enhanced business value to clients.

Walid is currently serving as a team member assisting the special compliance coordinator for Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd, appointed by the US Department of Commerce, to report on compliance with US export control laws and regulations. He is also serving as lead project manager assisting the auditor appointed by the US Environmental Protection Agency to report on corporate compliance of Volkswagen AG with respect to its settlement terms with the EPA, US Department of Justice and various states.

Nicholas Galbraith
Barnes & Thornburg LLP

Nick Galbraith is an associate in the Washington, DC office of Barnes & Thornburg. He has a wide range of international trade experience. He counsels clients on US export controls and sanctions laws, including drafting compliance policies and procedures; export classifications; licensing requirements under the International Traffic and Arms Regulations, the Export Administration Regulations and US sanctions maintained by the Office of Foreign Assets Controls; and the disclosure of potential violations to relevant authorities.

He is a member of the team assisting the Special Compliance Coordinator appointed by the US Department of Commerce to monitor, assess and report on the US export control compliance of Zhongxing Telecommunications Equipment Corporation, of Shenzhen, China, and ZTE Kangxun Telecommunications Ltd of Hi-New Shenzhen, China (collectively, ZTE).

In addition, Nick assists companies in their efforts to meet the demands of an ever-evolving regulatory environment, including the assessment of developments related to Iran, Russia, the Ukraine and Venezuela.

Nick's trade remedies experience includes petitions for the imposition of antidumping and countervailing duties, administrative reviews and scope ruling requests, as well as otherwise advising companies on the potential applicability and impact of such duties. He assisted an organic chemicals company in obtaining the imposition of over 400 per cent combined countervailing and antidumping duties on subject imports from China.

Nick also advises clients on other import and customs issues, including product classifications and obtaining customs ruling letters, safeguard actions, and Section 301 duties. Moreover, he is involved in the trade-related aspects of mergers and acquisitions, including voluntary filings before the Committee on Foreign Investment in the United States and mandatory notifications to Directorate of Defense Trade Controls.

Adetayo Osuntogun
Barnes & Thornburg LLP

Adetayo 'Tayo' Osuntogun is an associate in the Washington, DC office of Barnes & Thornburg. Tayo is a member of the international trade practice group where he advises business and institutional clients on international trade law, including export controls, economic sanctions, trade remedies, trade policy and customs and import regulations. He

works regularly with government agencies that regulate international trade to help clients realise their distinct objectives surrounding their global commerce initiatives.

Tayo represents clients before various federal agencies such as the Bureau of Industry and Security, the Directorate of Defense Trade Controls, the Office of Foreign Assets Control, US Customs and Border Protection, US International Trade Commission and the International Trade Administration. His experience in export controls and economic sanctions includes assisting clients with commodity jurisdictions, export classifications, licensing, drafting and revising compliance policies and procedures to meet the demands of an ever-shifting regulatory environment, as well as assisting clients with export classifications. Tayo provides clients with counselling, licensing services and enforcement representation with respect to US economic sanctions, anti-boycott regulation and CFIUS.

Tayo's practice also encompasses US Customs regulations on imports, including Section 301 and Section 232 tariffs, antidumping and countervailing duties, product marking and country of origin issues, tariff classification, valuation, free trade agreements and trade preference programmes. He resolves complex free trade agreement verifications, seizures, voluntary disclosures and penalties. Tayo has successfully pursued binding rulings, regulatory changes and petitions.

Tayo is a member of the team assisting the Special Compliance Coordinator appointed by the US Department of Commerce to monitor, assess and report on the US export control compliance of Zhongxing Telecommunications Equipment Corporation, of Shenzhen, China and ZTE Kangxun Telecommunications Ltd of Hi-New Shenzhen, China (collectively, ZTE).

Barnes & Thornburg LLP
1717 Pennsylvania Avenue NW
Suite 500
Washington, DC 20006-4623
United States
Tel: +1 202 289 1313
adetayo.osuntogun@btlaw.com
nicholas.galbraith@btlaw.com
www.btlaw.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