THE GUIDE TO SANCTIONS

FOURTH EDITION

Editors
Rachel Barnes KC, Paul Feldberg, Anna Bradshaw, David Mortlock, Anahita Thoms, Wendy Wysong and Ali Burney

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK
© 2023 Law Business Research Ltd
www.globalinvestigationsreview.com

No photocopying: copyright licences do not apply.

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 was accurate as at September 2023, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-256-7

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

Acknowledgements

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

Akrivis Law Group, PLLC

Baker & Hostetler LLP

Baker McKenzie

Barnes & Thornburg LLP

BDO USA, PA

Bonifassi Avocats

Cravath, Swaine & Moore LLP

Dechert LLP

Eversheds Sutherland

Forensic Risk Alliance

Global Law Office

Jenner & Block LLP

Linklaters LLP

McGuireWoods LLP

Miller & Chevalier Chartered

Navacelle

Peters & Peters Solicitors LLP

Ropes & Gray LLP

Steptoe & Johnson

Sullivan & Cromwell LLP

Three Raymond Buildings

Willkie Farr & Gallagher LLP

Publisher's Note

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

When this Guide was launched, I wrote that we were living in a new era for sanctions: more countries were using them, with greater creativity and (occasionally) self-centredness. I had no idea how true this statement would prove to be. Recent events have supercharged their use, to the point where sanctions never sleep. And that was before Russia invaded Ukraine . . .

Sanctions have become everybody's go-to tool. And little wonder. They are powerful; they reach people otherwise beyond reach. They are easy – they can be imposed or changed at a stroke, without real legislative scrutiny. And they are cheap for governments (as in the cost of making them versus their wider impact); once they exist, others do all the real heavy lifting.

It is on the heavy lifting part where this book can help. The pullulation of sanctions regimes, and sanctions, has created day-to-day headaches and challenges for all nearly all businesses 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.

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 should help them to do so even better. Whoever you are, we are confident this book has something for you.

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* and our new book on money-laundering and anti-money laundering regimes.

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
September 2023

Foreword

The term 'sanctions' is not new. The 90s have been called the 'decade of sanctions' of the UN Security Council. Today we are observing the unprecedented expansion of economic, financial, trade, cyber, targeted, individual and other types of sanctions (restrictive measures) applied by states and regional organisations unilaterally without the authorisation of the UN Security Council. Compliance with unilateral sanctions is enforced by multiple tools, including secondary sanctions exposure, criminalisation of sanctions circumvention and maximum pressure campaigns. Pecuniary penalties as a result of civil charges, even after securing settlement agreements with the US Office of Foreign Assets Control, may reach billions of US dollars.

Complicated, confusing and overlapping sanctions regulations, the proliferation of penalising mechanisms, the high risk and severity of penalties, unclear, lengthy, costly and complicated licensing procedures, uncertainties around the scope of humanitarian carve-outs, broad interpretations of the sanctions regimes, complications in delisting procedures and high legal costs all heighten risks and result in the growing de-risking and over-compliance by all actors in sanctioning, sanctioned and third countries.

It is a principled position of the mandate that any unilateral measures can only be taken by states and regional organisations without the authorisation of the UN Security Council if they fully correspond to criteria of countermeasures or retortions under the law of international responsibility. Any other measures qualify as unilateral coercive measures and are illegal under international law. These unilateral measures, independent of their legality, also have enormous humanitarian effects, which are often neglected or considered to be unintended by the sanctioning parties.

At the same time, as a Special Rapporteur I receive multiple complaints not only about the direct impact of sanctions but also often of over-compliance with all types of sanctions for many, if not all, of the reasons stated above.

De-risking and over-compliance have negative effects on all nationals or residents of countries under sanctions, often involving discrimination on the grounds of nationality, place of birth, residence, registration, IP address or any other nexus with these countries. It results in the isolation of countries, their companies and individuals, breach of trade and cooperation networks, and creates challenges to, or uncertainties of, access to justice and to remedies for those affected, and thus a lack of accountability.

I can also cite the detrimental effects on all basic human rights arising from impediments to the delivery of goods that are not subjected to sanctions, including those that are explicitly exempted from sanctions regimes via humanitarian carve-outs, such as food, medicine, fertilisers, medical equipment and spare parts, as well as many other goods necessary for the maintenance and development of critical infrastructure, thus rendering humanitarian provisions de facto almost non-existent. Financial institutions, manufacturers and delivery and insurance companies refer to broad and unclear interpretations of sanctions limitations by states or the compliance sector. They also mention the risks involved in delivering goods that may be perceived as 'dual use' (relevant to many types of medicine, rescue equipment and even simple consumer goods such as toothpaste), the impossibility or challenges of bank transfers, insurance or deliveries due to other elements of sanctions regulations, or the simple risk-aversion by refraining from dealing or cutting ties with any actor suspected of, or perceived as, having relations with the country under sanctions.

In particular, multiple reports refer to the challenges of delivering humanitarian assistance to the countries under sanctions even in the course of global public health crises, including the covid-19 pandemic, or epidemics (dengue), or in the aftermath of natural disasters such as earthquakes. They also refer to sanctions-induced challenges of effectively implementing humanitarian resolutions of the UN Security Council. Over-compliance and its serious adverse impact on humanitarian work persist even after the adoption of specific, targeted and often time-limited humanitarian carve-outs, such as those adopted for Syria by the US, UK and EU in response to its catastrophic earthquakes in February 2023 (UN Security Council Resolutions 2664 and 2615).

Information about the scope of international and unilateral sanctions, counter-sanctions, legal regimes of different countries, and legal assessment of, and challenges in, litigation in sanctions cases is often fragmentary or politicised. As a Special Rapporteur I very much welcome reflections and open dialogue on

all aspects relevant to sanctions and their impact, as well as discussions about mechanisms to ensure protection of the rights of all those affected by unilateral measures, analyses on the various challenges pertaining to humanitarian carve-outs and licensing, and mechanisms of litigation, accountability, responsibility and redress.

In terms of the serious practical implications of international and unilateral sanctions, compliance and over-compliance, I believe that the experience and views of practitioners exposed in *The Guide to Sanctions* will contribute to the international ongoing debate around the above-mentioned and other relevant issues.

Alena Douhan
UN Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights
September 2023

CHAPTER 22

The Role of Forensics in Sanctions Investigations

Leilei Wu, Bridget Johnson, Christine Sohar Henter and Michelle Rosario[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 law enforcement by the Office of Foreign Assets Control (OFAC), the US Department of Justice and other regulatory 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 transactions designed to circumvent economic sanctions. The

---

1 Leilei Wu is a senior manager and Bridget Johnson is a manager at BDO USA, PA. Christine Sohar Henter is a partner and Michelle Rosario is a law clerk at Barnes & Thornburg LLP. The authors would like to acknowledge the contributions of Linda Weinberg and Roscoe Howard, partners at Barnes & Thornburg LLP, and Nicole Sliger, Anthony Lendez and Pei Li Wong, partners at BDO USA, PA.

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 a sanctions compliance programme (SCP) or enhancing or testing an existing one.

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 effective 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 and 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 to take into consideration any changes in the organisation. A properly designed risk assessment and testing and auditing cycle should minimise exposure in the event of an apparent violation. Moreover, 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 overall risk assessment and compliance efforts.

---

2 See https://ofac.treasury.gov/media/16331/download?inline.

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-U.S. or U.S. 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 U.S. sanctions program objectives, and were large or sophisticated organizations.'

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. In addition, 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 non-compliance by employees.

Key forensic procedures and analytical tools

Data analysis

Among the most effective investigative procedures applied in testing or investigating as part of an SCP is a statistical analysis of historical and 'real-time' transactional data. It is critical for a company to be able to 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 analyses can be performed to help identify and thwart sanctions violations. The following observations from recent enforcement cases (as discussed in more detail in 'Analysis of recent enforcement cases – a forensics focus' below) could further inform efforts to prevent and detect potentially suspicious activities.

- Use keyword search terms 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

4 31 C.F.R. Part 501, Appendix A, at www.ecfr.gov/current/title-31/subtitle-B/chapter-V/part-501/appendix-Appendix%20A%20to%20Part%20501.

keywords on these communications, including metadata reviews (e.g., to/from fields). These tools can also analyse system access logs to identify users who accessed the system and can then obtain internet protocol (IP) addresses and GPS coordinates of the users. Further, a company can proactively use keyword search terms across communication channels in the normal course of business to identify suspect transactions or 'code' words in real time and block those communications.

- Anticipate potential compliance risks, especially when entering new business areas, and leverage data and IT systems to automatically block transactions that violate US sanctions. For example, companies engaging in overseas transactions for the first time should proactively identify risks, including the potential for current business partners and the countries in which they operate to become subject to future sanctions. Data analytics can flag transactions and use controls such as automated restricted-party and restricted-country screening, IP address blocking and SWIFT payment analyses to prevent illegal payments, travel, shipments and services in restricted regions. Additionally, companies can improve the effectiveness of IT controls by ensuring data is complete, standardised and used consistently across the enterprise.
- Test and assess IT controls periodically to ensure they remain effective in preventing compliance violations. Compliance control breakdowns can occur as the result of weak or out-of-date algorithms that, for example, can allow close matches to Specially Designated Nationals lists to evade filters, flagged payments to be released without review or failures to flag IP addresses in sanctioned regions. For example, companies can apply text analytics and natural language processing to detect fuzzy matches. OFAC may consider a company's failure to review and improve its compliance procedures to be an aggravating factor in prosecuting compliance violations.
- Require supporting documentation for travel, shipment and payment requests to be submitted through IT approval systems, allowing automated flagging of transactions. Making it mandatory to attach supporting documents to system approval requests, such as employee expense receipts related to travel and entertainment and bills of lading related to invoices, forces requestors and approvers to substantiate the veracity of dates, locations and entity names entered into the approval system. IT systems can then perform automated matching on the verified information. For example, hotel locations supported by lodging bills can be compared to the requested travel destination to verify that travel was not to unapproved or sanctioned regions, and destinations from bills of lading can be compared to invoices to verify that deliveries and

payments did not go to entities other than those on the approved invoices. These controls also leave audit trails that are helpful in detecting trends and isolating questionable transactions.

- Verify accuracy and completeness of customers' data, including their branch information. While customers can be incorporated outside of sanctioned countries, they could maintain branches in sanctioned countries. Companies should consider requesting a complete list of branches, including all the name variations and physical addresses, from each of their customers and conducting additional due diligence on each branch. Data analysis should be considered as a way to identify discrepancies between the actual shipping addresses/payers' names and the documented data of the customer and its branches. Companies can also consider adopting master data management to standardise naming and addresses and facilitate the discrepancy analysis.
- Conduct sanctions-related due diligence prior to acquisitions. Sanctions-related due diligence is critical before acquisition of any entity, especially if the acquisition target is outside the US. Conducting interviews with all levels of employees could help companies to understand the acquisition target's compliance culture and assess employees' knowledge related to sanctions. Companies should also consider analysing all the available data at the acquisition target to detect any potential violation. Identifying violations or potential violations can help companies to voluntarily self-disclose as soon as possible and plan for targeted change in the acquisition targets' compliance governance.
- Automate and customise the training courses received by domestic and international employees. All relevant employees should have the same basic level of awareness in sanctions-related laws and regulations. Companies should consider providing online training courses with exams. Exam-scoring patterns can be analysed so companies can develop customised training programmes for employees at different subsidiaries. For example, international employees may benefit from training courses developed in the local language and extra introductory courses on US laws and regulations.
- Analyse leads from business partners for potential violations. Employees may instruct business partners to modify or hide certain details related to day-to-day transactions, such as shipments, payments and cash receipts, to circumvent compliance controls. Companies should provide channels such as dedicated email addresses, mailboxes and hotlines for business partners to report potential violations. Adopting natural language processing to analyse voice and text received should be considered as a course of action. Companies can check the leads from different channels with the internal structured and unstructured data and verify the authenticity of the leads.

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 desk 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, forensics 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. Investigators can consider using a case tool to consolidate and analyse all the open-source data. 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 conducting business directly or indirectly with sanctioned countries or regions or whose activities benefit sanctioned governments or sanctioned parties.

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, and the United Arab Emirates and Iran. 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, the US Treasury Department or other regulatory authorities.

The investment made to develop 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, a growing number of companies 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 the exponential growth of international transactions, reliance on manual compliance controls alone can no longer effectively protect organisations against costly enforcement actions or other risks associated with sanctions violations.

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.

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. In-person observation of body language can also be very valuable, 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, in-person 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 'in-person' 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 workarounds 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, the Myanmar military coup in 2021 and the Russian invasion of Ukraine in 2022. 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. Advanced 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 because of travel constraints that were 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 generally have a limited view when a mobile device is used and the person who holds the mobile devices can manipulate what can be viewed by investigators. Investigators need to be aware of these pitfalls when conducting remote procedures and may want to consider using an independent third-party observer physically on-site when possible. A keen awareness of relevant data protection or privacy laws and regulations, state and commercial secrecy laws and employment regulations is key to successful remote interviews and inspections.

For remote interviews, interviewers should be alert to the possibility of other individuals in the same room who may be listening in or coaching the interviewee. 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 to 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.

Data preservation and collection activities are major activities in an investigation. Forensics 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 these devices and is often challenging and slow, especially in times when global logistics services are overextended; for example, during the covid-19 pandemic.

Many organisations still rely heavily on hard copy documentation to conduct business. Often, the need to maintain a hard copy paper trail is 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 on-site examination of the original hard-copy

documentation whenever possible. Companies should consider digitising the hard copies used in the business processes and managing the digitised data for easy retrieval and analysis.

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 helps reduce misunderstandings 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 is 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 any 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 adjustments to the configuration of 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, internal discussions and employee evaluations. 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 future violations.

Action plans should include identification of responsible parties, follow-up timelines, and procedures with features, such as scheduled action plan updates; retraining or retesting of employees; follow-up sampling of transaction activity to test controls; updated or enhanced risk assessments; and 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 offers 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.

Godfrey Phillips India

On 1 March 2023, Godfrey Phillips India (GPI), a tobacco manufacturer based in Mumbai, India, settled this case[6] with a payment of US$332,500. GPI used the US financial system to receive payments totalling approximately US$360,000 for tobacco it indirectly exported to North Korea in 2017. For the US financial institutions to fulfil the transactions, GPI used several third-country intermediary parties to obscure the connection with North Korea, causing US financial institutions to clear the payments. In an email exchange, GPI employees also decided not to include 'North Korea' or the North Korean customer's details on any trade document, but merely referenced the intermediary with a third country as the generic destination.

The case demonstrates the importance of comprehensive compliance programmes for foreign entities engaging in financial transactions processed through US financial institutions. Robust compliance programmes can help foreign entities understand potential US sanctions risks. The case also highlights the importance of companies using keyword search terms across communication channels to identify and suspend suspicious transactions promptly. Finally, it emphasises the necessity to implement effective compliance training, which keeps employees updated on the rapidly changing risk environment.

Payward, Inc

Payward, Inc (doing business as Kraken), a Delaware incorporated global virtual currency exchange, agreed to pay US$362,158.70 to settle this case[7] in November 2022. Kraken's platform allows users to buy, sell or hold cryptocurrencies, trade those currencies for fiat currency or exchange one cryptocurrency for another. Although Kraken maintained controls designed to prevent users from opening an account while in a sanctioned jurisdiction, it did not implement similar IP address blocking on transactional activity facilitated on its platform,

6 See https://ofac.treasury.gov/recent-actions/20230301_33.

7 See https://ofac.treasury.gov/recent-actions/20221128.

which caused Kraken to process 826 transactions totalling approximately US$1.6 million on behalf of users residing in Iran in apparent violation of the Iranian Transactions and Sanctions Regulations. After identifying this problem, Kraken implemented automated blocking for IP addresses linked to sanctioned jurisdictions and adopted multiple blockchain analytics tools to assist in sanctions compliance.

This case illustrates the importance of using geolocation tools, including IP address blocking and other location verification tools, to identify and prevent illegal transactions in restricted regions. It also demonstrates the importance of regular internal auditing and testing to identify deficiencies in existing compliance policies. Another lesson from this case is that a company should implement robust remedial measures after becoming aware of potential sanctions issues and the shortcomings of data analysis tools and analytics, then commit to continuous sanctions compliance investments as technology evolves.

CA Indosuez (Switzerland) SA and CFM Indosuez Wealth

CA Indosuez (Switzerland) SA (CAIS) and CFM Indosuez Wealth (CFM) are both indirect subsidiaries of Credit Agricole Corporate and Investment Bank. In September 2022, CAIS and CFM agreed to settle their potential civil liability for approximately US$750,000 and US$400,000, respectively, for apparent violations of Cuba, Iran, Syria, Ukraine-related and Sudan sanctions programmes.[8] CAIS and CFM's compliance procedures included collecting customers' data for know-your-customer purposes, which includes address information revealing the location of account holders that reside in sanctioned countries. Despite having this data, from April 2013 to April 2016 CAIS processed a total of 273 transactions (security procurements and commercial transactions), totalling over US$3 million through US banking correspondents, on behalf of the 17 individuals located in Iran, Syria, Sudan, Cuba and the Crimea region of Ukraine. Similarly, CFM also failed to address the known risks from December 2011 to 2016 by allowing 11 individuals residing in Iran, Syria and Cuba to conduct 426 transactions (security procurements and commercial transactions) worth over US$1.2 million. Although both companies implemented internal restrictions designed to prevent certain payments to persons residing in sanctioned regions, they later discovered that their internal restrictions did not prevent securities-related payments from being made to certain accounts. CAIS and CFM later implemented measures to prevent these payments.

8 See https://ofac.treasury.gov/recent-actions/20220926_33.

This case highlights the importance of integrating customer data into companies' compliance screening process to ensure all collected information informs compliance. It also demonstrates the value of testing and auditing controls to identify gaps in controls and compliance policies, and proactively implementing remedial actions.

Banco Popular de Puerto Rico

Banco Popular de Puerto Rico (BPPR), a Puerto Rican bank with branches in Puerto Rico and the Virgin Islands, settled its potential civil liability with OFAC for processing over 300 transactions totalling over US$850,000 on behalf of two low-level government of Venezuela employees in apparent violation of Venezuela-related sanctions in May 2022.[9] On 5 August 2019, Executive Order (EO) 13884 blocked property and interests in property of the Venezuelan government, which included:

- 'any political subdivision, agency, or instrumentality';
- 'any person owned or controlled, directly or indirectly', by the Venezuelan government; and
- 'any person who has acted or purported to act directly or indirectly for or on behalf of' any government entity.

EO 13884 was incorporated into the amended Venezuela Sanctions Regulations (VSR) on 22 November 2019.

Shortly after the issuance of EO 13884, BPPR began reviewing accounts that might be affected by the Order, but it took the bank 14 months to block four personal accounts of two customers employed by the government of Venezuela. When EO 13884 was announced, BPPR identified one customer working in the Diplomatic Representation Office of the Venezuelan government and the other account holder employed by a Venezuelan state-owned entity. BPPR's delay in identifying these customers resulted in the processing of 337 prohibited transactions totalling US$853,126, which violated the VSR. With OFAC's consideration of the aggravating and mitigating factors, BPPR agreed to a settlement payment of over US$255,000.

This case illustrates to financial institutions the importance of taking swift action following the issuance of new sanctions-related prohibitions. While BPPR had documentation of the customers' government connections, the company did not block the accounts for more than a year after the Executive Order was issued.

9 https://ofac.treasury.gov/recent-actions/20220527_33.

To be more agile to an evolving regulatory risk environment, companies should proactively surface key information from documents, such as government relationships, and convert this data into a structured format. Having this information readily available enables companies to perform timely due diligence and respond more rapidly to government sanctions.

Toll Holdings Limited

An international freight forwarding and logistics company headquartered in Australia, Toll Holdings Limited, settled more than 2,000 apparent violations of multiple OFAC sanctions programmes by agreeing to pay a settlement of over US$6 million.[10] For six years, from January 2013 to February 2019, Toll was involved in nearly 3,000 payments related to shipments involving three sanctioned countries – specifically, North Korea, Iran and Syria. Some of these payments also involved the property or interests of property of an entity on OFAC's Specially Designated Nationals and Blocked Persons List. Both types of payments were processed through at least four financial institutions in the US or through foreign branches of US-based financial institutions and totalled approximately US$48 million.

Toll had expanded rapidly through acquisition, and, as a result, the business included numerous legacy freight forwarding companies in regions around the world. Notably, by 2018, Toll had nearly 600 different IT systems spread across its business. The sanctioned activity was commonly initiated by Toll's overseas units, altogether comprising 23 different Toll entities across Asia, Europe, the Middle East and North America. During its normal course of operations, Toll engaged in complex payment practices, such as making or receiving payments for multiple shipments in a single invoice or spreading one shipment across multiple invoices. In these cases, the value of the payment amount associated with a sanctioned country or entity could be a portion of a larger amount comprised of both sanctioned and non-sanctioned parties.

Around May 2015, some Toll personnel were put on notice that the subject payments were in potential violation of US sanctions regulations when one of its banks restricted a Toll subsidiary's use of its US account after identifying a transaction with Syria. However, despite instruction from its compliance office that Toll must not be involved with any shipments to US-sanctioned jurisdictions, the activity continued, and it was not until years later that Toll implemented 'hard controls' to block these illegal shipments and payments. These controls included

10 https://ofac.treasury.gov/recent-actions/20220425.

disabling the country and location codes for ports and cities to or from sanctioned countries in its freight management system, thereby preventing its shipments from transiting in sanctioned countries.

This enforcement action emphasises the necessity for companies to continually examine the effectiveness of their internal controls as their business expands and the crucial role that IT systems play in ensuring compliance. While Toll had compliance policies, sanctioned activity was able to occur in part due to lack of system controls. While policies are a necessary aspect of a compliance programme, companies should also regularly assess whether those policies can be 'hard coded' as part of their IT system configuration. Furthermore, companies should use data analytics to continually monitor the transactional activity that flows through these systems to identify any compliance concerns and address sanctions risks in a timely manner.

British American Tobacco plc

OFAC's largest-ever settlement with a non-financial company was with British American Tobacco plc (BAT), an English tobacco and cigarette manufacturer that agreed to pay over US$500 million to settle alleged violations of sanctions against North Korea.[11] BAT established an elaborate payment scheme for approximately US$250 million in over 200 payments from a North Korea joint venture, through blocked bank accounts in North Korea to BAT's Singaporean subsidiary, which implicated US banks clearing the transactions between 2009 and 2016. BAT's apparent violations occurred because the US-dollar-denominated payments for its exports of tobacco to the North Korean Embassy in Singapore cleared through the US financial system.

The penalty was the maximum statutory civil amount permitted (e.g., twice the value of the sum of transactions), reflecting OFAC's finding that these apparent violations were egregious and not voluntarily disclosed. The main lesson from this case is that companies that knowingly engage in conspiracies that cause US persons to be involved in prohibited transactions, including dealing with blocked persons, risk receiving severe penalties. Further, without a culture of compliance driven by senior management and suitable compliance policies and controls, which must be reassessed when regulations evolve, these companies have heightened risk for potential violations.

11 https://ofac.treasury.gov/recent-actions/20230425.

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: 'If you think compliance is expensive, try non-compliance.'[12] 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 remembering that OFAC considers 'good faith' compliance efforts in the disposition of enforcement matters. OFAC 'will consider favorably subject persons that had effective SCPs at the time of an apparent violation'.[13] 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.

OFAC's advice 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 dos and don'ts, from a forensics perspective, for building an effective 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 sanctions concerns; and
- enforce policies and procedures, and identify, document and remediate weaknesses.

12 Rodney T Stamler, Hans J Marschdorf and Mario Possamai, *Fraud Prevention and Detection: Warning Signs and the Red Flag System* (Routledge, 2014), p. 4.

13 See https://ofac.treasury.gov/media/16331/download?inline.

Due diligence and screening:

- conduct due diligence on customers, distributors, suppliers, contractors, logistics providers, financial institutions and other partners;
- use and test automated screening software continuously, being cognisant of filter faults – prioritise alerts by severity and tune configuration of the software as needed;
- 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; and
- establish anonymous reporting channels for employees and policies to ensure non-retaliation for whistle-blowing.

Testing and auditing:

- assess tools, technology and data needed to monitor sanctions compliance;
- consider artificial intelligence to detect red flags – calibrate and test routinely;
- 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; and
- 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 could 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.

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

This, alas, creates complication for the rest of us. Hitherto no book has addressed the complexities that businesses and their advisers must address by dint of this proliferation in a structured way. GIR's *The Guide to Sanctions* fills that gap. 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, and is an invaluable resource.

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

ISBN 978-1-80449-256-7