GIR Global Investigations Review

The Guide to Sanctions - Sixth Edition

The role of forensics in sanctions investigations

The Guide to Sanctions - Sixth Edition

As the geopolitical landscape continues to be unsettled, sanctions are becoming the go-to response from many states and are being applied in ever more innovative ways. This naturally creates a host of issues from the perspective of international businesses – and the practitioners who advise them.

Edited by Rachel Barnes of Three Raymond Buildings, Anna Bradshaw of Peters and Peters, Paul Feldberg of Brown Rudnick, David Mortlock of Willkie Farr & Gallagher, Anahita Thoms of Baker & McKenzie and Wendy Wysong of Steptoe, the sixth edition of ***The Guide to Sanctions*** is an invaluable resource as it dissects the topic in a practical fashion from every stakeholder's perspective.

Generated: July 10, 2025

The role of forensics in sanctions investigations

Meghan Fiore, **Nathalie Terrazas**, **Christine Sohar Henter** and **Luis F Arandia**

Barnes & Thornburg LLP

BDO

Summary

INTRODUCTION

The global economy relies heavily on cross-border transfers of funds, goods and services, which are increasingly subject to economic sanctions administered and enforced by the US Department of the Treasury's Office of Foreign Assets Control (OFAC), among other regulatory authorities. As a result, investigations involving potential sanctions violations are becoming more prevalent as these regulatory authorities and enforcement agencies continue to use sanctions as a tool to influence foreign behaviour and mitigate national security risks.

Entities seeking to circumvent sanctions regulations often undertake elaborate measures to obfuscate their business activities from counterparties and/or avoid detection by government agencies. These illicit actors may disguise transactions through complex payment processes, shell corporations, subsidiaries or other methods that exploit the intricacies of global transactions and financial instruments to hide the true source and use of funds, goods or services. To prevent and detect such sanctions violations and mitigate regulatory risk, organisations should implement effective sanctions compliance programmes and investigate indicators of potential violations. Leveraging innovative investigative techniques and tools, along with consultants possessing specialised forensic knowledge, is critical to implementing these compliance programmes, conducting investigations, and ensuring the efficacy and sustainability of sanctions compliance programmes.

This chapter outlines the principal investigative methodologies and best practices employed by forensics professionals in sanctions investigations and highlights analytical tools to uncover facts and patterns in complex transactions designed to circumvent economic sanctions. This chapter presents a combination of best practices, published guidance from OFAC and examinations of recent regulatory enforcement actions to help explain the evolving sanctions environment. And it aims to support forensic and compliance professionals in developing and enhancing a sanctions compliance programme (SCP).

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 the United States or with 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, such as risk assessments and compliance testing, are critical elements of effective compliance measures. This chapter focuses on the two SCP components most relevant to forensics – risk assessment and testing and auditing – and their interplay with the factors OFAC considers in administrative enforcement actions.[3]

The risk assessment and testing and auditing components of an SCP should be developed in tandem and should inform each other as the business activities and regulatory landscape of an organisation shift over time. Every organisation is unique, and the risk assessment and testing and auditing plans implemented should be tailored to fit its specific business operations. Additionally, risk assessments should be refreshed periodically to account for changes in an organisation, especially those that significantly impact an organisation's

risk profile. A properly designed risk assessment and testing and auditing cycle should be dedicated to minimising an organisation's regulatory exposure in the event of an apparent violation. Moreover, conclusions drawn from testing and auditing should be analysed and used to inform the company's overall risk assessment and compliance efforts. If testing and auditing reveal that risks are higher than anticipated in one portion of the business, these results should be integrated into the company's overall compliance strategy. Benchmarking testing and auditing results over time is also crucial for analysing trends and evaluating the effectiveness of the SCP. By systematically comparing current and past results, organisations can identify patterns, measure improvements and detect areas requiring further attention. This ongoing analysis not only helps in understanding the evolving risk landscape but also ensures that the SCP remains robust and responsive to new challenges. Regular benchmarking allows for the continuous refinement of compliance strategies, ensuring they are both effective and aligned with the organisation's risk profile.

When determining the appropriate administrative action in response to a sanction's violation, OFAC will consider certain 'general factors' described in its Economic Sanctions Enforcement Guidelines.[4] During the testing and auditing process, these factors should be the focus of the risk assessment evaluation. According to the OFAC guidelines, a risk assessment should involve evaluating several factors, such as customers, products, services, supply chain, intermediaries, counterparties, transactions and geographical locations. The extent of the assessment required will depend on the organisation's size, nature and sophistication.

Implementing a testing and auditing plan as part of a risk-based SCP will reduce an organisation's risk of committing a sanctions violation and is often a mitigating factor when enforcement agencies determine the penalties to levy against violators. 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 being dedicated to minimising instances of aggravating conduct. For example, audits 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. A company must be able to identify potentially suspicious transactions and determine the 'who, what, where, when and how' by establishing a timeline of events.

Statistical data analysis is an invaluable tool to analyse data ranging from basic pivot-table analysis to more advanced software applications. It helps to stratify, synthesise and flag data from various systems. The key to using data analysis effectively is linking transactional evidence buried in data fields from disparate sources to identify hidden relationships or correlations. It is also important to incorporate procedures to check the veracity of data that is being relied upon.

Artificial intelligence (AI) has emerged as a powerful tool in sanctions-related investigations. AI technologies are increasingly being used to enhance data analysis capabilities. These technologies can automatically detect patterns and anomalies in large datasets, which might be indicative of sanctions violations. AI can also help in predicting potential risks by analysing historical data and identifying trends.

Data analytic tools, now often enhanced with AI capabilities, are useful in conducting robust forensic analyses to help prevent and detect sanctions violations. Recent enforcement cases have provided valuable insights that can aid in identifying and preventing potentially suspicious activities. Further details on these cases can be found in the section 'Analysis of recent enforcement cases – a forensics focus'.

BEST PRACTICES TO IDENTIFY AND PREVENT SUSPICIOUS ACTIVITIES

Evidence of prohibited transactions is often found in unstructured data (e.g., electronic communications, such as email, voicemail and instant messages). Forensic tools can identify suspicious activity using keywords in these communications, including metadata reviews (e.g., timestamp information, geolocation data and network information). These tools can also analyse system access logs to identify users who accessed the system and obtain their internet protocol (IP) addresses and global positioning system coordinates. Further, companies can pre-emptively deploy keyword search terms across communication channels or other unstructured data in the normal course of business to identify suspect transactions or 'code' words in real-time and block those communications.

Potential compliance risks should be anticipated, especially when expanding into new business areas, and it is optimal to leverage data and information technology (IT) systems to automatically block transactions that violate US sanctions. For example, companies engaging in overseas transactions for the first time should identify risks, such as the possibility of current business partners or the countries they operate in becoming 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. To improve the efficacy of IT controls, companies should ensure that data is complete, standardised and used consistently throughout the enterprise.

IT controls should be tested and assessed periodically to ensure they remain effective in preventing compliance violations. Compliance control breakdowns can occur due to weak or outdated algorithms that, for example, allow close matches to specially designated nationals (SDCs) lists to bypass filters, release flagged payments without review, or fail to flag IP addresses in sanctioned countries and regions. Organisations should dedicate adequate resources to identifying and remediating these deficiencies. For example, organisations can apply text analytics and natural language processing to detect partial or similar matches (i.e., fuzzy matches) between transacting parties and entities and individuals listed on sanctions lists. OFAC may consider a company's failure to review and improve its compliance procedures and IT controls as an aggravating factor in prosecuting compliance violations.

Organisations should make it mandatory for employees to submit supporting documentation for travel, shipment and payment requests through IT approval systems, allowing automated flagging of high-risk transactions. Requiring supporting documents to be attached to system approval requests – such as employee expense receipts for travel and entertainment, and bills of lading related to invoices – makes it easier for requestors and approvers to verify the accuracy of the information entered into the system, including dates, locations and entity names. IT systems can then perform automated matching on the verified information. For example, hotel locations supported by lodging bills can be compared with the requested travel destination to verify that travel was not to unapproved or sanctioned regions. Also, destinations from bills of lading can be compared against invoices

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

The accuracy and completeness of customers' data should be verified, including their subsidiary and branch information. While customers may be incorporated outside sanctioned countries, they could also maintain subsidiaries or branches in sanctioned countries. Companies should consider requesting a complete list of subsidiaries and branches, including all name variations and physical addresses, from each of their customers and conducting additional due diligence on each entity. Data analysis should be considered to identify discrepancies between the actual shipping addresses or payers' names, and the documented data of the customer and its subsidiaries and branches. Companies can also consider adopting master data management to standardise naming and addresses to facilitate the discrepancy analysis.

Sanctions-related due diligence should be conducted before acquisitions, especially if the acquisition target operates outside the US. Conducting interviews with employees at various levels will help organisations understand the acquisition target's compliance culture and assess employees' knowledge related to sanctions compliance. Companies should also consider analysing available data at the acquisition target to detect potential violations. Identifying violations or potential violations enables companies to voluntarily self-disclose as soon as possible and improve the acquisition targets' compliance governance.

Training courses provided to domestic and international employees should be automated and customised. All relevant employees should have the same basic level of awareness of sanctions-related laws and regulations. Employees in positions that are most exposed to sanctions risk, such as senior management and those processing significant transactions, should undergo advanced training. Companies should consider offering online training courses with a minimum threshold for exams. Exam-scoring patterns can be analysed to inform the development of customised training programmes for employees at different branches and subsidiaries. For example, international employees may benefit from training courses developed in the local language and extra introductory courses on US laws and regulations.

Tips from employees and business partners that allege potential violations should be investigated. Employees looking to circumvent compliance controls may instruct business partners to modify or hide certain details relating to daily transactions, such as shipments, payments and cash receipts. Companies should provide channels such as dedicated email addresses, mailboxes, and hotlines for employees and business partners to report potential violations. Adopting natural language processing to analyse voice and text messages received should be considered as an investigative strategy. Companies can check the tips from different channels with the internal structured and unstructured data and verify the authenticity of the tips.

INVESTIGATIVE DUE DILIGENCE

Investigative due diligence typically involves a set of research tools and approaches that can be applied to a wide range of investigations. In sanctions-related investigations, these tools may include:

- documents and electronic records disclosed by a party;

- public records gathered through open-source research or on-site searches; and
- observational site inspections or human source intelligence.

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 business registry details, litigation records, asset ownership details, news and publications, and social media) can help untangle the web of indirect relationships and interrelated connections involved in transactions. Investigators can use a case management tool to consolidate and analyse open-source data collected.

Although the investigative trail often begins with the company's books and records, suspected perpetrators often engage in a variety of techniques to cover their tracks, such as transaction 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 the ownership structure and executive leadership positions of complex organisational structures.

Violators may go to great lengths to obscure beneficial ownership of companies or disguise the beneficiaries of certain transactions. However, these patterns can often be identified through common elements, such as addresses, proxies or nominees in business structures, or law firms or accountants used to register companies. Investigators often use link analysis and other visualisation tools to track the information uncovered, map the networks of bad actors, and help companies understand their potential exposure to these bad actors. Identifying patterns or connections in large volumes of information requires tools to distil the information quickly and clearly into charts, graphs or other visualisations.

SUPPLY CHAIN MAPPING AND PREDICTIVE ANALYSIS

Forensic analysis tools enable the use of models for predictive analysis and present opportunities for mapping global supply chains. This mapping can identify the sanctions risk posed by third parties, including 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 parties.

Supply chains that extend to countries actively trading with sanctioned jurisdictions pose a higher sanctions risk. Primary examples of these relationships include Russia, Venezuela, China, North Korea, United Arab Emirates and Iran. To evaluate the potential third-party risk of such relationships, it is critical to establish a process that involves continually updating data analysis and models with the latest information from recent enforcement actions and published advisories from regulatory authorities, such as the US State Department and the US Treasury Department.

Investing in the development of a supply chain risk map can yield significant long-term benefits, particularly for large, complex companies with multinational presences. By mapping out the supply chain, parties can gain valuable insights into potential sanctions risks, which can then be used to develop effective internal controls, training programmes, and due diligence practices.

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 provide fourth-party or fifth-party logistics services[5] can enhance their existing contingency plans by incorporating sanctions risks into 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 sanction's designation or significant enforcement action. More and more companies are adopting predictive analytics to manage sanctions risk.

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 static or antiquated compliance controls alone can no longer effectively protect organisations against costly enforcement actions or other risks associated with sanctions violations.

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 to collected data or evidence, validating authenticity and confirming facts leading up to the recording of transactions. Observing body language in person can also be valuable, particularly in sensitive situations involving potential wrongdoing. Therefore, on-site interviews or inspections present unique opportunities for compliance personnel, investigators or those engaged in testing.

In practice, in-person interviews help investigators evaluate employees' knowledge of compliance policies and the effectiveness of training, which may shed light on documented decisions made by those employees. This can potentially distinguish intentional policy violations from decisions made because of inadequate training or human error. These 'in-person' meetings provide first-hand knowledge of how written policies and procedures are being executed. In some cases, disparities between the written procedure and its execution may expose gaps. Process walk-throughs can also identify when employees are taking shortcuts by skipping procedural steps. Additionally, interviewees can articulate why certain procedures were not followed and describe inefficiencies or pain points in the process, highlighting the need for policy updates or additional controls.

Field interviews and observations can also detect instances when compliance processes are not taken seriously by employees or management, or when they are not adequately supported due to a lack of 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 common, may resort to unapproved workarounds or off-system processes, resulting in incomplete system data and failure to apply controls.

Irrespective of geography, a prolonged crisis may cause significant business interruptions, such as high staff turnover or absenteeism. In situations where employees are unable to access their workplace due to civil unrest, natural disasters or other widespread disturbances, executing an SCP effectively can be challenging. In such situations, the knowledge or resources required to fully execute the SCP may not be available, and employees may feel increased pressure to ignore processes for the sake of business continuity. Events such as the covid-19 pandemic, the military coup in Myanmar in 2021 and Russia's invasion of Ukraine in 2022 are examples of such crises. Sanctions compliance

should influence the crisis response and business continuity plans for sophisticated, global organisations. Advanced planning and on-site walk-throughs help provide a clearer picture of potential risks, which may not be anticipated or detected during a crisis.

When on-site procedures cannot be performed due to restrictions such as travel constraints brought on by the covid-19 pandemic, remote interviews and inspections can be a satisfactory alternative if investigators adhere to best practices. Videoconferencing allows the interviewer to gauge the interviewee's body language and facial expressions, which can help establish rapport. Additionally, videoconferencing enables investigators to present documents on a shared screen. Mobile devices can be used to provide a view of facilities when an in-person inspection is impossible. But investigators must be cognisant of the limitations of mobile devices, as they provide a restricted view, and the person holding the mobile device may manipulate what is visible to investigators. Therefore, investigators are advised to exercise caution when using mobile devices and should consider having an independent observer physically present on-site.

During remote interviews, interviewers should be alert to the possibility of other individuals being present in the same room, listening in or coaching the interviewee. An interviewee may also try to avoid being interviewed or answering questions by claiming technical difficulties. Remote interviews also run the risk of being recorded surreptitiously. And a keen understanding 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.

Data preservation and collection activities are crucial 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 without being onsite may require shipping these devices. This process can be challenging and slow, especially during times when global shipping lanes are acutely affected by geopolitical conflicts.

Many organisations still rely heavily on physical documentation to conduct business. Often, the need to maintain a physical paper trail is driven by local government requirements and business norms in the country. Organisations may scan physical documents for electronic storage, but the quality of the scan is often inconsistent, and the scanned images are at risk of being altered. It is best practice to follow up with an on-site examination of the original physical documentation. Companies should consider digitising the hard copies used in business processes and managing the digitised data for easy retrieval and analysis.

One major limitation of remote procedures is the lowered ability to conduct unscheduled interviews or surprise spot checks. These cannot be performed remotely easily, mainly because of the coordination required to organise remote data collection, interviews or facility inspections. Ultimately, proper planning is key and communicating expectations to the subject entity or individual helps reduce misunderstandings over logistics. The investigations team should verify the preliminary results obtained through remote investigative procedures by conducting an in-person inspection if travel is feasible.

POTENTIAL POST-INVESTIGATION PROCEDURES

An investigation should conclude with a final report. Organisations can use the report's findings and recommendations to formulate action plans to address compliance

deficiencies that were identified. When gaps in compliance knowledge are revealed, the organisation should implement role-specific or targeted training. For example, if a finding shows that screening systems failed to detect name variations, adjustments to the configuration of the screening system may be necessary. But other findings may require enterprise-wide initiatives and policy development.

Specific compliance deficiencies uncovered through transaction analysis and forensic techniques, such as look-backs, are also useful for isolating incorrect compliance decisions and enhancing existing training programmes and materials. Understanding the root causes of these deficiencies is useful for forming situation-based questions and case studies for training materials, internal discussions and employee evaluations. Studying the various types of deficiencies may also help in creating automated system-generated policy reminders to guide 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, additional 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 should be 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 for demonstrating the application of various forensic investigative methods and best practices, while also highlighting practices that might have contributed towards the identification of mitigating factors considered by OFAC. As evidenced in the cases summarised below, the obligations of non-US persons in foreign jurisdictions to comply with US sanctions and export control laws are paramount, as highlighted by the issuance of a Tri-Seal Compliance Note by the DOJ, DOC and OFAC on 6 March 2024.[6] The absence of a comprehensive SCP can heighten the risks of potential sanctions violations.

VIETNAM BEVERAGE COMPANY

In October 2024, Vietnam Beverage Company Limited (VBCL) agreed to a settlement of US$860,000 to address potential civil liabilities related to apparent violations of OFAC sanctions on North Korea by two of VBCL's subsidiaries.[7] Between April 2016 and October 2018, VBCL's subsidiaries received around US$1.1 million in payments through US financial institutions for alcoholic beverage sales to North Korea, causing the export of financial services to North Korea by these US financial institutions.

In late 2017, VBCL acquired majority ownership in several Vietnamese alcoholic beverage companies, which had been exporting products globally, including to North Korea. Since 2016, these subsidiaries conducted export sales with payment terms requiring pre-delivery payment, invoicing in US dollars, and shipping from Vietnam. Contracts specified alcohol types and quantities, with deliveries sometimes split into multiple shipments under a single contract.

Between January 2016 and September 2018, the subsidiaries executed 26 contracts to sell alcoholic beverages to North Korea, involving two North Korean entities and two third-party

companies in Singapore and the Seychelles. This resulted in 47 invoices and 43 wire transfers totalling over US$1 million, processed through US banks. Payments were made by 15 third-party companies from Hong Kong, China, Turkey, Singapore and the Seychelles on behalf of North Korean entities. Nearly all the associated business documents for these dealings made specific references to North Korea and the receipt of payment in US dollars. At the time the misconduct occurred, neither VBCL nor its subsidiaries had sanctions compliance programmes related to US sanctions.

In December 2019, following certain management changes, VBCL's new leadership discovered these past dealings and immediately ceased further transactions with North Korea. Although VBCL did not file a voluntary self-disclosure, the company proactively notified OFAC of its internal findings through a letter, providing additional information regarding the conduct at issue. VBCL also implemented a comprehensive sanctions compliance programme modelled after OFAC's May 2019 Framework for Compliance Commitments. This included a directive against business with sanctioned jurisdictions, due diligence requirements, customer screening against sanctions lists, and the establishment of compliance teams. VBCL also engaged an independent third party for customer background checks and provided sanctions compliance training to its subsidiaries.

This case demonstrates how non-US persons in foreign jurisdictions may face sanctions liability, especially when utilising the US financial system. As noted in the Tri-Seal Compliance Note, OFAC has actively employed its enforcement authorities against foreign persons who have, among other things, caused US persons (like US financial institutions) to violate OFAC sanctions, conspired to do so, indirectly exported services from the United States, or otherwise engaged in violative conduct. Like the case here, the Tri-Seal Compliance Note provided an example of OFAC enforcement when a non-US person routes a prohibited transaction through the US or the US financial system, thereby causing a US financial institution to process the payment in violation of OFAC sanctions.

This enforcement action also highlights that not having a risk-based sanctions compliance programme raises the likelihood of sanctions violations, even for foreign companies. Companies should design and implement a programme tailored to their size, sophistication, business operations, partners and consumer base. Companies should also be cautious of successor liability and conduct thorough due diligence, especially during mergers or acquisitions involving overseas business activities, to identify preexisting compliance risks and deficiencies. This includes evaluating the geographic locations of customers, supply chains, intermediaries and counterparties as part of a comprehensive risk assessment to identify potential interactions with OFAC-prohibited entities.

MONDO TV, SPA

In June 2024, Mondo TV, Spa (Mondo), an Italian animation firm, agreed to pay US$538,000 to resolve potential civil liabilities related to violations of OFAC sanctions against North Korea.-[8] From May 2019 to November 2021, Mondo transferred approximately US$538,000 to a studio owned by the North Korean government for animation outsourcing services. The wire transfers were processed through US financial institutions, and Mondo inadvertently involved them in transactions that dealt with blocked property interests of the North Korean government, violating US sanctions.

Mondo had been subcontracting animation work to the Scientific Educational Korea Studio (SEK), a North Korean government-owned firm, since the 1990s. This collaboration involved

communication between Mondo's senior management and SEK representatives in North Korea and Europe. Mondo also hosted SEK animators in Italy for training sessions.

By 2019, Mondo owed SEK more than US$1.1 million for various projects. In July 2019, they agreed to settle this debt through monthly instalments for work completed before 2016, when Mondo paused their collaboration due to human rights concerns, and for new projects starting in 2019. Under the 2019 agreement and new agreements thereafter, SEK issued invoices to Mondo which identified that payments should be directed to third-party companies in China and the United States, along with their associated banking information at several US financial institutions. Mondo then remitted payments to these companies, seemingly to settle SEK's debts with these entities.

During its relationship with, and when remitting the payments to the intermediaries identified by SEK, Mondo appeared to understand they were ultimately paying a North Korean company. Documents associated with the transactions, including contracts, invoices, payment receipts and email communications, explicitly referenced North Korea. Mondo lacked a sanctions compliance policy at the time.

This case emphasises the need for robust compliance frameworks and proactive measures to ensure adherence to international sanctions. Companies should conduct thorough risk assessments and enhanced due diligence on business partners, customers and third-party intermediaries to identify links to sanctioned parties. They should verify the ultimate beneficiaries of transactions and ensure transparency in financial dealings.

Additionally, companies should monitor transactions and financial flows of funds by implementing transaction monitoring systems to detect unusual or suspicious activities that may indicate sanctions violations. Reviewing payment instructions and financial flows of funds are essential to ensure they do not involve sanctioned entities or jurisdictions. Furthermore, using sanctions screening tools and integrating screening processes into the organisation's operations, with regular updates, can help safeguard against potential sanctions violations.

Finally, this case is an additional example of how non-US persons in foreign jurisdictions may face sanctions liability, especially when utilising the US financial system.

SCG PLASTICS CO. LTD

In April 2024, SCG Plastics Co., Ltd. (SCG Plastics), a Thai trading company that sells plastic resin products, settled with OFAC for US$20 million over 467 apparent violations of Iran sanctions.[9] From 2017 to 2018, SCG Plastics facilitated US$291 million in wire transfers through US financial institutions for Iranian-origin high-density polyethylene resin (HDPE), produced by Mehr Petrochemical Company (Mehr), a joint venture based in Iran involving SCG Plastics' parent company, SCG Chemicals and the National Petrochemical Company of Iran (NPC).

From 2009 to July 2018, SCG Plastics resold 60 per cent of Mehr's HDPE output to East Asian manufacturers. To receive payments for the HDPE, SCG Plastics used deceptive shipping and documentation practices to obscure the Iranian origin of the products. Invoices instructed customers to remit US dollar payments to SCG Plastics' Thai bank accounts, processed by US correspondent banks. SCG Plastics listed 'Middle East' or 'Jebel Ali, UAE' as the origin in shipping documents, avoiding mention of Iran. SCG Plastics also transhipped the

HDPE through the UAE, where the company's shipping agent issued shipping documentation indicating UAE as the port of loading, instead of Iran.

Additionally, SCG Plastics paid debts owed by Mehr to third-party vendors based in Iran and other countries in US dollars at least 10 times in exchange for HDPE produced by Mehr. This allowed Mehr to access the international financial system and engage in trade by not disclosing to financial institutions that the payments were on behalf of Mehr, an Iranian entity. SCG Plastics misleadingly labelled these payments as 'payment for goods', despite not purchasing goods from these vendors. When dealing with Iranian vendors, Mehr instructed SCG Plastics to pay into bank accounts held by non-Iranian companies in other countries, further concealing the Iranian parties' involvement and facilitating Iran's covert trade through US financial institutions.

This case highlights that deliberately concealing the involvement of sanctioned individuals or countries in transaction documentation can lead to significant penalties. SCG Plastics misrepresented the origin of goods, mischaracterised payments and diverted shipments with falsified shipping documents to effectively disguise transactions involving Iranian entities.

Implementing a comprehensive, risk-based SCP is essential. This includes appointing dedicated compliance officers, conducting regular training and performing audits to ensure adherence to sanctions regulations. Companies should perform enhanced due diligence on all parties involved in transactions, including third-party intermediaries, to identify links to sanctioned entities or jurisdictions. They should also verify the accuracy and completeness of shipping and payment documentation to ensure transparency. The Middle East region is known to be a high-risk transhipment area known for evasive transportation activities, which calls for enhanced due diligence and compliance measures to manage the associated risk.

AIOTEC GMBH

Aiotec GmbH, a Germany-based company focusing in sourcing industrial equipment for the energy sector, settled for US$14,550,000 in December 2024 for a single apparent violation of OFAC sanctions on Iran.[10] Aiotec indirectly sold and supplied an Australian polypropylene plant to Iran via a US company and processed payments through US financial institutions between 2015 and 2019.

An Australian company hired a US company to facilitate the sale of a decommissioned polypropylene plant. On 27 November 2015, Aiotec entered into a sales agreement with the US company to purchase the plant for US$9.7 million. The agreement specified that Aiotec would not resell the plant 'to any country, person, or entity or for shipment to any destination, which is subject to sanctions or embargo by US Government'. On 26 October 2015, Aiotec signed an end-user certificate indicating that the plant would be shipped to Turkey, intending to operate it as a joint venture with a Turkish company. But on 29 November 2015, Aiotec executed an agreement to sell the plant to Petro-Iranian Downstream Industries Development Co. (PIDID) and transport it to Iran.

Between 2017 and 2019, Aiotec began exporting plant components to an Iranian port, facilitated by two freight forwarders. These freight forwarders were instructed to refrain from registering the end user's name and address as Iran, opting instead to list either the UAE or Turkey. In 2016 and 2017, Aiotec issued two additional end-user certificates, asserting that the end-user was a Turkish company. In 2017, the general counsel for the US company requested that Aiotec reaffirm their commitment to refrain from shipping the

plant to any destination subject to sanctions. Moreover, in 2017, Aiotec presented details of a fictitious agreement between Aiotec and a Turkish company concerning the division of responsibilities.

On 22 August 2018, the US company received a copy of the first page of the agreement between Aiotec and PIDID from an anonymous source, leading to the suspension of Aiotec's access to the plant, which was still undergoing dismantlement in Australia. In September 2018, the US company issued a letter to Aiotec regarding the breach of the sales agreement due to the exportation of the plant to Iran and requested the bills of lading for these exports. Aiotec denied the authenticity of the PIDID agreement and provided bills of lading that falsely indicated the parts were re-exported from the UAE to Turkey, along with a copy of the fraudulent strategic relationship agreement between Aiotec and the Turkish company, and a letter from the Turkish company falsely confirming their purchase of the plant. Consequently, the US company reinstated Aiotec's access to the plant, and the remaining parts were shipped to Turkey based on the provided false bills of lading. Aiotec continued to furnish false bills of lading to the US company, concealing the fact that the plant was exported to Iran or PIDID.

Despite the US company's best efforts to thwart the sale and/or export of the plant to a sanctioned country, they could not do so because of the deceptive documentation and collusion between Aiotec and the Turkish company. This case underscores the importance of thorough investigative due diligence in preventing and detecting sales or transactions involving sanctioned countries. For instance, leveraging public records for research or conducting in-person observations and/or site inspections could help. Additionally, companies should consider incorporating audit provisions into agreements with partners to ensure compliance and detect potential violations early in the process.

FAMILY INTERNATIONAL REALTY LLC

Family International Realty LLC, a real-estate company based in Miami, along with a US individual settled for US$1,076,923 in January 2025.[11] This settlement relates to the 73 apparent violations of OFAC's sanctions related to Ukraine and Russia. The individual and Family International Realty attempted to circumvent OFAC's Ukraine/Russia-related sanctions by transferring nominal ownerships of three luxury condominiums, originally owned by two Russian oligarchs, to non-sanctioned family members and shell companies controlled by those family members.

When Valeri Abramov was added to OFAC's SDN List on 26 January 2018, the individual, with the help of a law firm, transferred ownership of the condominium from joint marital property to Mr Abramov's spouse to conceal his interest in the unit. Family International Realty LLC subsequently received a commission for the sale of this condominium in March 2019, amounting to US$1.2 million. The firm was reimbursed for expenses incurred by the individual in maintaining the property.

In a similar circumstance, Viktor Perevalov was added to the SDN List on 26 January 2018. Following Mr Perevalov's guidance, the individual sought to remove his name from the property title for two condominium units in South Florida. With help from a law firm, the individual established a Delaware shell company and transferred nominal ownership of Mr Perevalov and his spouse's condominium units to this entity. The shell company was owned by Mr Perevalov's minor children and managed by the individual. Upon completion of the transfer, the individual rented out the two units as luxury hotel accommodations on

approximately 64 occasions between 2018 and 2023, generating approximately US$840,254 in rental revenue. Family International Realty LLC earned commission from the rental activities of Mr Perevalov's condominium units.

This case underscores the critical role of gatekeepers in the context of sanctions compliance. Gatekeepers include realtors, investors, attorneys, and trust and business service providers, who may facilitate the evasion of sanctions because they provide critical business services. It is imperative for gatekeepers and financial institutions collaborating with such entities to conduct thorough due diligence to ensure that gatekeepers are not assisting or acting on behalf of sanctioned parties.

Employing investigative due diligence to discern patterns and connections through shared elements – such as addresses, proxies, law firms or accountants – can reveal critical information about the parties engaged in the activity. Open-source data, including public records, asset ownership and social media, can shed light on these interconnected relationships.

SANCTIONS COMPLIANCE: BEST PRACTICES AND LESSONS LEARNED

At a 2023 conference, former US Deputy Attorney General for the US Department of Justice, Lisa Monaco made the following remarks about the importance of sanctions enforcement: 'What was once a technical area of concern for select businesses should now be at the top of every company's risk compliance chart.'[12] 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 favourably subject persons that had effective SCPs at the time of an apparent violation.'[13] But it is difficult to predict how OFAC will apply this principle to individual cases. As such, compliance professionals and organisational leaders should not assume their efforts will result in the mitigation of penalties.

OFAC's advice in the 'Framework for OFAC Compliance Commitments', 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 these cases, 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 PROGRAMMES

- conduct comprehensive, risk-based compliance assessments;
- implement clear, risk-based 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.

DUE DILIGENCE AND SCREENING

- conduct KYC due diligence processes on customers, end users, distributors, suppliers, contractors, logistics providers, financial institutions and other partners;

- use and continuously test automated screening software, being cognisant of filter faults – prioritise alerts by severity and adjust the software's rules as needed to improve its performance and accuracy;
- develop systems to track movement of goods and financial transactions from manufacturing to ultimate end users;
- deploy blockchain and distributed ledger technologies to improve due diligence records;
- understand diversion and circumvention risk;
- monitor recent enforcement actions for effects on operations;
- establish anonymous reporting channels for employees and business partners, and implement policies to ensure non-retaliation for whistleblowing; and
- leverage IP blocking and geolocation screening tools to remain compliant in industries with emerging technologies and complex global transactions.

TESTING AND AUDITING

- assess tools, technology and data needed to monitor sanctions compliance;
- consider using 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 (e.g., mergers, acquisitions and management changes);
- execute supply chain audits with country-of-origin verification; and
- perform supplier and distributor audits.

DON'T . . .

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

CONCLUSION

Sanctions compliance continues to grow in importance as does its impact on the programmes, tools and talents of legal, compliance and forensics professionals. The international political trends and criminal activities that drive the use of sanctions show no signs of disappearing, while worldwide economic instability continues to reveal vulnerabilities in the global economy.

Establishing a robust and proactive SCP can provide significant 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 feel confident that these efforts will pay off in the long term.

ENDNOTES

[1] Meghan Fiore and Nathalie Terrazas are senior managers at BDO USA, PC. Christine Sohar-Henter and Luis Arandia, Jr. are partners 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 and Pei Li Wong, principals at BDO USA, PC.

[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-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 organisation's management, caused significant harm to US sanctions program objectives, and were large or sophisticated organisations.'

[4] Code of Federal Regulations (CFR), Title 31, Part 501, Appendix A, at eCFR; Appendix A to Title 3, Part 501 – Economic Sanctions Enforcement Guidelines.

[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.

[6] See https://ofac.treasury.gov/media/932746/download?inline.

[7] See https://ofac.treasury.gov/media/933501/download?inline.

[8] See https://ofac.treasury.gov/media/932986/download?inline.

[9] See https://ofac.treasury.gov/media/932841/download?inline.

[10] See https://ofac.treasury.gov/media/933661/download?inline.

[11] See https://ofac.treasury.gov/media/933941/download?inline.

[12] See www.justice.gov/archives/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national.

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

Christine Sohar Henter christine.sohar-henter@btlaw.com
Luis F Arandia luis.arandia@btlaw.com

https://btlaw.com/

Read more from this firm on GIR

Meghan Fiore mtoohey@bdo.com
Nathalie Terrazas nterrazas@bdo.com

https://www.bdo.com/

Read more from this firm on GIR