THE GUIDE TO SANCTIONS

THIRD EDITION

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

The Guide to Sanctions

Third Edition

Editors

Rachel Barnes QC

Paul Feldberg

Nicholas Turner

Anna Bradshaw

David Mortlock

Anahita Thoms

Rachel Alpert

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2022
For further information please contact insight@globalinvestigationsreview.com

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

www.globalinvestigationsreview.com

ISBN 978-1-83862-874-1

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 LLP

Carter-Ruck

Cravath, Swaine & Moore LLP

Eversheds Sutherland

Fangda Partners

Forensic Risk Alliance

Global Law Office

Jenner & Block LLP

McGuireWoods LLP

Mayer Brown

Miller & Chevalier Chartered

Navacelle

Peters & Peters Solicitors LLP

Seward & Kissel

Simmons & Simmons LLP

Steptoe & Johnson

Stewarts

Three Raymond Buildings

White & Case LLP

Willkie Farr & Gallagher LLP

Publisher's Note

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

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

Sanctions have truly become a go-to tool. And little wonder. They are powerful; they reach people who would otherwise be beyond our reach. They are easy – you can impose or change them at a stroke, without legislative scrutiny. And they are cheap (in the simplest sense)! It's up to others once they're in place to do all the heavy lifting.

The heavy lifting part is where this book can help. The pullulation of sanctions regimes, and sanctions, has resulted in more and more day-to-day issues for business and their advisers.

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

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*.

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

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

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

David Samuels
Publisher, GIR
June 2022

Contents

Foreword

I am delighted to welcome you to this third edition of Global Investigations Review's *The Guide to Sanctions*. The international, geographical, political, criminal, legal and regulatory elements that make up sanctions programmes ensure that this will remain one of the most complex compliance areas facing practitioners. The following chapters contain important information, advice and best practice for sanctions and export controls as a compliance discipline, courtesy of some of the world's leading legal, forensic and compliance specialists. The daily change to the international regimes requires practitioners and businesses to be constantly monitoring and horizon-scanning across all relevant jurisdictions, and the Guide is packed full of resources that will enable readers to do just that.

The current sanctions environment makes this Guide a must read for any practitioner who manages or advises on sanctions compliance. This Guide is the work of leading industry specialists who have all given their time and expertise to produce a resource that should be on every bookshelf. At a time of growing complexity, readers may find the Guide worthy of being constantly consulted as a valuable reference resource, not only in its own right, but also for the treasure trove of links and references to information and guidance provided by the regulators who guide industry in implementing sanctions policy.

Sanctions never sleep, and since the previous version of this Guide, we have seen the UK settle into an autonomous programme and increased international coordination with major countries and blocs looking to align as closely as possible. The US is no longer the only major player.

The sanctions regimes in place for countries such as Iran, Syria, North Korea and Yemen, to name just a few, have continued to evolve, but the focus since August 2021 has been squarely on Russia and Belarus. This Guide will bring you

up to date with the significant changes in those regimes, as at the time of writing, covering both the sanctions and export controls, as well as updating you on the developments in other regimes, including China and Hong Kong.

As with earlier editions, this third edition covers the major sanctions programmes from the United Nations, the United States, the European Union, the United Kingdom and the Asia-Pacific region, including the types of prohibitions imposed by the relevant programmes, the licence procedures and the measures that are available to challenge listings. Each of the major jurisdictions has an enforcement section that details the process and elements of enforcement from the relevant jurisdiction. The Guide also covers the re-emergence of thematic sanctions programmes; no longer limited to terrorism and narcotics, these programmes have seen a significant growth over the past few years. The third edition welcomes new authors who share their experiences representing sanctioned clients, among others.

The section on compliance programmes will enable readers to review their own programmes against best practice and improve and enhance their own controls if required. The final section covers sanctions and export controls in practice, giving good advice on how to navigate international, extraterritorial and often conflicting requirements of global sanctions and export control rules.

It is important to remember that financial crime is not a competition and that we make the biggest impact when we work together across industry and governments. The partnerships and collaboration across the globe play an important part in managing international sanctions. Part of my role at UK Finance is to liaise with industry and governments to help promote public–private partnerships and ensure that we are all fighting financial crime, especially in the sanctions space, as a coordinated and collaborative network of specialists, in the UK and elsewhere.

The Guide to Sanctions is intended to enable readers to be a valuable part of the sanctions and export controls community, dedicated to fighting financial crime and helping to protect our wider society from the impacts of those that seek to cause harm on the international stage.

Neil Whiley
Director of Sanctions, UK Finance
June 2022

Part II

Compliance Programmes

CHAPTER 16

Sanctions Screening: Challenges and Control Considerations

Charlie Steele, Gerben Schreurs, Sarah Wrigley, Deborah Luskin and Jona Boscolo Cappon[1]

Background

Economic sanctions have evolved in complexity over time. Total embargoes were formerly common, and were enacted to completely block trade with disfavoured countries. List-based sanctions were later introduced, specifically targeting people and entities rather than entire countries. The most well-known list-based sanctions are those maintained by the US, published in the Office of Foreign Assets Control's (OFAC) Specially Designated Nationals and Blocked Persons (SDN) List.[2] More finely targeted sanctions result in fewer unintended collateral consequences than embargoes but are often more difficult to comply with. Screening against targeted sanctions lists presents considerable challenges, given the complex corporate structures used to obscure underlying sanctioned parties, the inherent difficulties in name matching, and difficulties in screening for entities that are, directly or indirectly, 50 per cent or more owned in the aggregate by sanctioned parties, under OFAC's 50 Percent Rule.

An example of increasing complexity are sanctions that address both entities and their underlying activities. For example, the US sectoral sanctions[3] introduced in 2014 in response to Russia's annexation of Crimea target certain specified sectors of the Russian economy (especially energy, finance and armaments), prohibiting

1 Charlie Steele and Gerben Schreurs are partners, Sarah Wrigley and Jona Boscolo Cappon are directors and Deborah Luskin is an associate director at Forensic Risk Alliance.

2 https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.

3 https://home.treasury.gov/system/files/126/ukraine_eo3.pdf.

certain types of activity by US persons with identified individuals or entities operating in those sectors. More recently, following Russia's invasion of Ukraine in 2022, there were additional sectoral sanctions imposed, which limit specific investment activities, among other things, with Russian entities.[4] This new type of sanctions added another level of complexity to compliance. Existing challenges in correctly identifying sanctioned parties were compounded by the requirement to also understand the nature of the proposed transaction by the customer.

Sanctions screening failures have figured prominently in a number of OFAC penalty settlements with both financial institutions and non-financial entities. To this end, we discuss current regulatory guidance for a successful sanctions screening programme, how screening relates to the core elements of the overall sanctions compliance programme, examples of enforcement actions focusing on screening failures, and screening in the context of a sanctions investigation.

Regulatory expectations for sanctions screening

In the US, OFAC has not published detailed guidance regarding expectations for sanctions screening programmes. The US Department of the Treasury's 2019 'A Framework for OFAC Compliance Commitments' (the Framework),[5] after addressing five high-level elements for a sound sanctions compliance programme, identifies 10 common root causes of sanctions compliance failures. The sixth root cause addresses some of the failures that occur due to poor configuration of sanctions screening software.[6] The guidance mentions some specific failings, including using outdated screening lists, incomplete data screening and not accounting for alternative spellings of names. These are a few of the potential points of failure when screening for possible sanctions targets, but there are several more that we discuss in this chapter.

---

4 https://home.treasury.gov/system/files/126/new_debt_and_equity_directive_3.pdf.

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

6 'VI. Sanctions Screening Software or Filter Faults: Many organisations conduct screening of their customers, supply chain, intermediaries, counterparties, commercial and financial documents, and transactions in order to identify OFAC-prohibited locations, parties, or dealings. At times, organizations have failed to update their sanctions screening software to incorporate updates to the [Specially Designated Nationals And Blocked Persons] List or [Sectoral Sanctions Identifications] List, failed to include pertinent identifiers such as SWIFT Business Identifier Codes for designated, blocked, or sanctioned financial institutions, or did not account for alternative spellings of prohibited countries or parties – particularly in instances in which the organisation is domiciled or conducts business in geographies that frequently utilize such alternative spellings (i.e., Habana instead of Havana, Kuba instead of Cuba, Soudan instead of Sudan, etc.).'

In 2015, OFAC published a one-page guidance document regarding the management of 'false hits' lists.[7] Pursuant to that guidance, where companies have determined that potential sanctions match alerts can be disregarded as false positives and suppressed going forward to avoid unnecessary review time, compliance personnel should be involved in oversight and administration of the lists, and, among other things, the lists should be modified promptly and as necessary to account for changes to sanctions lists.

In contrast to the limited guidance from OFAC, the New York Department of Financial Services (NYDFS), which regulates financial institutions licensed within the state of New York, has taken a more prescriptive stance as to sanctions screening programmes. The NYDFS has identified weaknesses in transaction monitoring and sanctions screening programmes within regulated institutions. It attributed these failures to insufficient governance and accountability at senior levels. As a result, the NYDFS set out specific requirements for these programmes[8] that require boards of directors or senior officers to certify compliance on an annual basis.[9]

The first compliance findings were due in April 2018 and required regulated institutions to:

- *Undertake comprehensive and holistic assessments of their transaction monitoring and sanctions filtering programs;*
- *Provide appropriate supporting evidence to demonstrate the effectiveness of the programs;*
- *Execute remedial efforts, material improvements, or redesigns to keep the programs in compliance; and*
- *Implement governance processes for the annual certification.*[10]

At a more detailed level, each regulated institution must maintain a sanctions screening programme that is reasonably designed to interdict transactions prohibited by OFAC and that includes the following attributes:

7 https://home.treasury.gov/system/files/126/false_hit.pdf.
8 Part 504 of the New York State Banking Regulations in 2017.
9 www.dfs.ny.gov/industry_guidance/transaction_monitoring.
10 New York State Banking Regulations.

- *Be based on the risk assessment of the institution;*
- *Be based on technology, processes or tools for matching names and accounts, in each case based on the institution's particular risks, and transaction and product profiles;*
- *End-to-end, pre- and post-implementation testing of the Filtering Program, including, as relevant, a review of data matching, an evaluation of whether the OFAC sanctions list and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and program output;*
- *Be subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the OFAC sanctions list and the threshold settings to see if they continue to map to the risks of the institution; and*
- *Include documentation that articulates the intent and design of the Filtering Program tools, processes or technology.*[11]

In addition, the sanctions screening programme must include:

- *Identification of all data sources that contain relevant data;*
- *Validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the Transaction Monitoring and Filtering Program;*
- *Data extraction and loading processes to ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems, if automated systems are used;*
- *Governance and management oversight, including policies and procedures governing changes to the Transaction Monitoring and Filtering Program to ensure that changes are defined, managed, controlled, reported, and audited;*
- *Vendor selection process if a third party vendor is used to acquire, install, implement, or test the Transaction Monitoring and Filtering Program or any aspect of it;*
- *Funding to design, implement and maintain a Transaction Monitoring and Filtering Program that complies with the requirements of this Part;*
- *Qualified personnel or outside consultant(s) responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis of the Transaction Monitoring and Filtering Program, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filings; and*

11 ibid.

- *Periodic training of all stakeholders with respect to the Transaction Monitoring and Filtering Program.*[12]

Although not all financial institutions are subject to these rules (and non-financial entities are not within their scope), they provide a useful benchmark in evaluating whether a sanctions screening programme has been designed well and is operating effectively.

In the UK, the Financial Conduct Authority's (FCA) Financial Crime Guide addresses compliance with sanctions and asset freezes.[13] In the context of a risk assessment, a firm should understand where sanctions risks reside, considering different business lines, sales channels, customer types and geographical locations, and should keep the risk assessment current. Examples of good practices related to sanctions screening include:

- *where a firm uses automated systems, these can make 'fuzzy matches' (be able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.);*
- *the firm should screen customers' directors and known beneficial owners on a risk-sensitive basis;*
- *where the firm maintains an account for a listed individual, the status of this account is clearly flagged to staff; and*
- *a firm should only place faith in other firms' screening (such as outsourcers or intermediaries) after taking steps to satisfy themselves that this is appropriate.*[14]

In addition to these examples of best practices, the Guide cites a £5.6 million fine by the FCA's predecessor against Royal Bank of Scotland (RBS) in 2010, where RBS failed to adequately screen its customers and payments against the sanctions list, did not ensure its 'fuzzy matching' remained effective, and, in many cases, did not screen the names of directors and beneficial owners of customer companies.

In addition to the OFAC, NYDFS and FCA regulatory guidance referenced above, the Wolfsberg Group, an association of 13 global banks, published 'Guidance on Sanctions Screening' in 2019.[15] The Guidance indicates that sanctions screening should be supported by key enabling functions, such as policies

12 ibid.

13 www.handbook.fca.org.uk/handbook/FCG.pdf.

14 id., at Section 7.2.3.

15 www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

and procedures, a responsible person, a risk assessment, internal controls and testing. These areas roughly correspond to the high-level pillars within OFAC's Framework. In addition to Wolfsberg's key enabling functions, the Guidance also discusses principles for generating productive sanctions alerts, the need for metrics and reporting, independent testing and validation, data integrity, and criteria used to develop screening technology in-house or to select a vendor to provide such services.

How sanctions screening fits into the sanctions compliance programme

Sanctions screening does not operate in a vacuum; it is an integrated piece of the sanctions compliance programme. In this section, we describe some of the key elements of an effective sanctions screening programme in relation to the five high-level areas of compliance articulated in OFAC's Framework.

Governance and risk assessment

When an entity implements proper governance and oversight and performs a sound sanctions risk assessment, there should be clear alignment between identified sanctions risks and the sanctions screening programme configuration. If the sanctions risk assessment determines that certain geographies, customers or products present significant sanctions risk, regulators would expect to see that the relevant sanctions lists are utilised for screening and that there are more stringent screening criteria applied in higher-risk areas.

For example, the NYDFS requires that attributes for sanctions screening programmes address links between the risk assessment and the screening programme configuration. Specifically, the tools used to screen for sanctions exposure must be based on the risk assessment, configured in a risk-based manner and tested to ensure they provide results in accordance with the identified risks; in addition, the entity must document links between risks identified and the configuration of the sanctions screening programme. This is an important reminder that entities should not just implement software to address general sanctions risks; rather, they should identify specific sanctions risks and then develop or procure software that sufficiently addresses those identified risks.

Internal controls – due diligence

To properly screen for potential sanctions violations, sufficient due diligence must be performed. During customer onboarding, the entity must obtain and verify key information to identify the customer, including, but not limited to, name, alternate names, address, date of birth, registration number and country of incorporation,

residence or nationality. These attributes are useful during subsequent sanctions screening as they help determine if a potential sanctions match is valid. The entity should also understand ultimate beneficial ownership (UBO) information, key trading partners and supply chain information, where relevant. UBO information, in particular, is relevant in determining if a person or company falls within the sanctions restrictions due to their beneficial ownership of a sanctioned entity. Before processing transactions, the company may need to understand the counterparty UBO, supply chain information, shipping information and mergers and acquisitions (M&A) due diligence information, including UBOs, controllers, goods and services and origin of goods. If insufficient due diligence is performed during onboarding and before transactions occur, it is difficult to have an effective sanctions screening programme in place later, when necessary and relevant information is not present with which to identify potential sanctions violations.

Internal controls – screening

Proper sanctions screening processes involve many controls. At a high level, we can consider three distinct phases: (1) inclusion of complete and accurate information; (2) the logic behind how matching occurs; and (3) how potential sanctions violations are evaluated.

The first consideration in sanctions screening is to determine if you have gathered all of the relevant information. This often involves collating siloed data across different business or product lines. It can also entail ensuring that all relevant information within those systems is included in the population of data for screening. In several recent OFAC enforcement actions, the agency noted absence of relevant data from the sanctions screening process.

- January 2022: Airbnb Payments Inc settled with OFAC for US$91,172 for processing payments for Cuba-related travel that was outside the approved categories. OFAC noted that neither guest country of residence and payment instrument information nor internet protocol (IP) addresses were gathered for sanctions screening.[16]
- November 2021: Mashreqbank psc, headquartered in the United Arab Emirates with a branch in London that processed US dollar payments, received a Finding of Violation from OFAC for failing to populate the originating institution field in their payment messages, such that originating

16 https://home.treasury.gov/system/files/126/20220103_abnb.pdf.

Sudanese financial institutions were not identified when sent to US financial institutions for processing.[17]

- April 2021: SAP SE, the global software provider, settled with OFAC for US$2,132,174 for providing software licences and related services to Iran. Internal audits conducted by SAP between 2006 and 2014 found that it did not screen customers' IP addresses, which limited its ability to determine the location where software was downloaded. OFAC identified the lag in addressing the lack of geolocation IP blocking as an aggravating factor in determining the settlement amount.[18]
- February 2021: BitPay, Inc settled with OFAC for US$507,375 for processing payments for over five years, where they possessed IP data and some invoice information that indicated the customer was located in a sanctioned jurisdiction, but did not utilise that information for sanctions screening.[19] As a result, customers with IP addresses or invoice information indicating origination in Crimea, Cuba, North Korea, Iran, Sudan and Syria were able to make purchases from merchants in the US and elsewhere using digital currency on BitPay's platform.
- December 2020: BitGo Inc settled with OFAC for US$98,830 for processing digital currency transactions for customers with IP addresses in numerous sanctioned jurisdictions.[20]

Of particular note, between July 2020 and January 2022, of the 30 settlements or Findings of Violation against companies, OFAC mentioned the lack of screening IP addresses in seven.[21] Although there is no regulation that requires IP address screening, it is clear from the regulatory feedback, including recent guidance,[22] that this is expected as part of a successful sanctions screening programme.

After all relevant information is gathered, the quality of the data must also be addressed. For example, typing errors, non-standard inputs, blank values and inconsistent structure can all impede effective sanctions screening.

The second consideration is the configuration of the sanctions screening programme. There are many areas to consider when defining the configuration, but we focus on the importance of an effective name-screening process.

---

17 https://home.treasury.gov/system/files/126/20211109_mashreq.pdf.
18 https://home.treasury.gov/system/files/126/20210429_sap.pdf.
19 https://home.treasury.gov/system/files/126/20210218_bp.pdf.
20 https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
21 Airbnb Payments, NewTek, Payoneer, SAP, BitPay, BitGo and Amazon.
22 https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

Sanctions screening can be performed against standing data within an entity or against transactions. The most common type of sanctions matching is based on name screening, determining whether there is a match between the sanctions list entry and a company's internal information. This is performed, for example, during due diligence on new customers, when due diligence is periodically refreshed, when transactions occur and during M&A activity. Name screening can generate both false-negative and false-positive matches.

False positives occur when names of non-sanctioned entities or individuals are incorrectly matched and flagged as sanctioned. Sanctions screening can reduce false positives and validate matches by leveraging the many attributes included in sanctions lists for individuals, companies, ships, aeroplanes and financial institutions. Sanctions lists typically contain several different pieces of identifying information, such as aliases, street addresses, dates of birth, nationalities, passport numbers, tax identification numbers, email addresses, corporate registration numbers, aircraft tail numbers, vessel registration identification numbers, website addresses and digital currency addresses.

However, the risk of false negatives – that is, failure to identify a true match to a sanctioned party – is much higher than the risk of false positives. A common problem occurs when screening looks only for exact matches, and therefore misses a potential match due to a slight variation in the name. Name variations can occur for a number of reasons, such as the presence of hyphens, use of titles, punctuation, spelling errors, use of initials, acronyms, name reversals, phonetic spellings, abbreviations and shortened names.

Language differences, phonetic transcriptions and transliteration from one alphabet or writing system to another further complicate the landscape of name matching. For example, a lack of standards for the spelling of Cyrillic names in Roman script introduces at least a dozen name variations for the former Russian leader Boris Yeltsin, ranging from Jelzin to Eltsine.

'Fuzzy matching' introduces flexibility in how the screening system matches names and terms. For example, 'Jon' and 'John' might be considered equivalent in a fuzzy matching system, particularly where the last name or date of birth is an exact match. However, the more expansive the fuzzy match criteria become, the greater the risk that the company will become inundated with false positives, which affects the effectiveness and efficiency of the screening process as a whole.

Configuration of fuzzy matching is both art and science. There are many data analytic methods to employ in fuzzy matching, such as sound methods (which use algorithms to turn similar sounding names into the same key to identify similar names), distance methods (which measure the difference in characters between two names), statistical similarity methods (which look at large data sets to train

the model to find similar names) and hybrids of these methods. A detailed analysis of the various methods is outside the scope of this chapter, but the more important point is that there is a regulatory expectation that fuzzy matching techniques will be employed and continually fine-tuned to address each company's unique environment and sanctions risk.

In recent years, several OFAC enforcement actions have noted fuzzy match inadequacies, including the following.

- July 2021: Payoneer Inc's US$1,385,901 settlement with OFAC noted several screening failures, including 'weak algorithms that allowed close matches to SDN List entries not to be flagged by its filter'.[23]
- April 2021: MoneyGram Payment Systems, Inc's US$34,328 settlement with OFAC cited, among other things, the company's 'fuzzy logic failures'.[24]
- September 2020: Deutsche Bank Trust Company Americas' September 2020 settlement with OFAC cited, among other things, the company's complete lack of fuzzy matching for names.[25]
- July 2020: Amazon.com Inc settled with OFAC for US$134,523 for Amazon's screening processes, which did not flag orders with address fields containing an address in 'Yalta, Krimea' for the term 'Yalta,' a city in Crimea, nor for the variation of the spelling of Crimea.[26] It also failed to interdict or otherwise flag orders shipped to the Embassy of Iran located in third countries. Moreover, in several hundred instances, Amazon's automated sanctions screening processes failed to flag the correctly spelled names and addresses of persons on OFAC's SDN List.
- November 2019: Apple settled with OFAC for US$466,912 for failing to identify that SIS, an App Store developer, was added to the SDN List and was therefore blocked.[27] Apple later attributed this failure to its sanctions screening tool's failure to match the upper-case name 'SIS DOO' in Apple's system with the lower-case name 'SIS d.o.o.' as written on the SDN List. The term 'd.o.o.' is a standard corporate suffix in Slovenia identifying a limited liability company.
- October 2019: General Electric Company (GE) settled with OFAC for US$2,718,581 for accepting payments from an entity on the SDN List.[28] The

23 https://home.treasury.gov/system/files/126/20210723_payoneer_inc.pdf.
24 https://home.treasury.gov/system/files/126/20210429_moneygram.pdf.
25 https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
26 https://home.treasury.gov/system/files/126/20200708_amazon.pdf.
27 https://home.treasury.gov/system/files/126/20191125_apple.pdf.
28 https://home.treasury.gov/system/files/126/20191001_ge.pdf.

sanctioned entity was Cobalt Refinery Company, or Corefco. The payments contained Cobalt's full legal entity name as it appears on OFAC's SDN List as well as an acronym for Cobalt (Corefco), but GE's sanctions screening software, which screened only the abbreviation of the SDN's name, never generated an alert on Cobalt's name.

All of the enforcement examples described above show that failures as to completeness of data and fuzzy matching can lead to ineffective sanctions screening and enforcement actions.

On a related note, one of OFAC's and the UK's Office of Financial Sanctions Implementation's (OFSI) 'mitigating factors' used to determine the final civil penalty amount is the strength of an entity's sanctions compliance programme, including the screening component. OFAC gave mitigation credit to several companies that implemented or improved their sanctions screening programmes after detecting violations, including the following.

- Sojitz (Hong Kong) Limited's January 2022 settlement with OFAC noted that the company revised its screening procedures to require all counterparties in all business transactions be subject to screening.[29]
- NewTek Inc's September 2021 settlement with OFAC noted that it implemented bulk name screening of product registrants and both current and pending distributors against the SDN List. In addition, it noted that the company implemented geo-IP blocking measures to prevent downloading or registering products from blocked locations.[30]
- First Bank SA's August 2021 settlement with OFAC noted that its remediation measures included updating its sanctions screening tool.[31]
- In a January 2021 settlement, OFAC noted that Union de Banques Arabes et Françaises now utilises the sanctions screening software used by its largest shareholder, which includes screening the client database, an anti-stripping module, negative news research, risk database research, vessel screening and country screening.[32]
- BitGo, Inc's December 2020 settlement with OFAC noted that the company now performs IP address blocking, as well as email-related restrictions for sanctioned jurisdictions, and performs periodic batch screening, reviews of

29 https://home.treasury.gov/system/files/126/20220111_sojitz.pdf.
30 https://home.treasury.gov/system/files/126/20210909_newtek.pdf.
31 https://home.treasury.gov/system/files/126/20210827_firstbank_flowers.pdf.
32 https://home.treasury.gov/system/files/126/01042021_UBAF.pdf.

screening configuration criteria on a periodic basis, screening all 'hot wallets'[33] against the SDN List, including cryptocurrency wallet addresses identified by OFAC, and a retroactive batch screen of all users.[34]

Finally, it is important to note that the examples thus far have focused on identifying matches for list-based sanctions targets. As noted above, there are other types of sanctions that are more targeted and complex – for example, OFAC's sectoral sanctions, which focus on entities and activities.[35] In 2019, Haverly Systems, Inc settled an OFAC enforcement action for US$75,375 after it invoiced JSC Rosneft, a Russian oil company, to be payable within 90 days.[36] The invoices were not paid within that time frame and this violated Directive 2 under the Russia sectoral sanctions, which, at the time of the transaction, prohibited dealing in new debt of greater than 90 days' maturity. Similarly, Standard Chartered Bank was fined over £20 million by the UK's OFSI for loans with maturity over 30 days to specific entities as part of the Ukraine sanctions.[37]

Another example is the recent ban on US-person investment in identified Chinese Military-Industrial Complex Companies (CMICs) on public exchanges; this involves identification of both the investor (are they a US person?) and the activity (does this transaction involve investment in or derivative of, or provide investment exposure to, securities in the specified CMICs?). As sanctions include more complex, targeted criteria, the methods needed to ensure compliance likewise become more complex, in some cases requiring companies to flag both the entity and the activity to determine whether potential sanctions violations have occurred.

OFAC's 50 Percent Rule adds an additional element to screening complexity. Under this Rule, any entity owned in the aggregate, directly or indirectly, 50 per cent or more by one or more blocked persons is itself considered blocked, and therefore subject to the same sanctions as the owners are.[38] This Rule means that screening may require tools that review and assess an entity's ownership structure, and do not just stop at a review against designated parties' lists. The difficulty in applying the 50 Percent Rule is evident in the recent designation of numerous Russian oligarchs with large, complex business holdings. As in 2014,

33 Cryptocurrency wallets that are online and connected in some way to the internet.
34 https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
35 https://home.treasury.gov/system/files/126/ukraine_eo3.pdf.
36 https://home.treasury.gov/system/files/126/20190425_haverly.pdf.
37 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.
38 https://home.treasury.gov/system/files/126/licensing_guidance.pdf.

when some Russian oligarchs were added to sanctions lists after the annexation of Crimea, they have employed various methods such as signing over assets to close relatives, registering entities in secrecy havens and creating nominee shareholders to evade detection through the 50 Percent Rule.

The Wolfsberg Group's sanctions screening guidance contains a discussion regarding the assessment of which data elements to screen.[39] Specifically, the guidance states:

> *Names of parties involved in the transaction are relevant for list based sanctions programmes, whereas addresses are more relevant to screening against geographical sanctions programmes and can be used as identifying information to help distinguish a true match from a false match. Other data elements, such as bank identification codes, may be relevant for both list and geographically based sanctions programmes.*
>
> *In a sanctions context, some data elements are more relevant when found in combination with other attributes or references. For example, detection of sectoral sanctions risk typically requires detection of multiple factors, such as those where both the targeted parties and the prohibited activities are involved. Many controls may not be capable of detecting both factors simultaneously and, therefore, may not be effective.*

Internal controls – virtual currency screening

There is incentive for heavily sanctioned countries, such as North Korea, Iran and Russia, to use cryptocurrency to evade sanctions. However, recent analysis indicates that cryptocurrency transactions indicating sanctions evasion have remained a relatively small portion of transactions received by illicit addresses, although the use of cryptocurrency is growing.[40]

OFAC's SDN List includes cryptocurrency addresses that should be blocked.[41] In practice, enforcement of the block relies on compliant cryptocurrency exchanges. If cryptocurrency is transferred with a non-compliant exchange or peer-to-peer, it likely will not be blocked.

Blockchain analysis has indicated that the majority of cryptocurrency transactions related to sanctions evasion were subsequently transferred to centralised exchanges.[42] OFAC sanctioned two non-compliant Russian-based exchanges,

---

39 www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

40 'The 2022 Crypto Crime Report', Chainalysis, February 2022.

41 OFAC FAQ 563.

42 ibid.

Chatex and Suex, accusing them of providing money-laundering services and adding them to the SDN List in 2021.

The methods used to identity sanctions evasion via cryptocurrency include screening for: the cryptocurrency addresses on the SDN List; addresses associated with those same blocked addresses; addresses associated with known exchange hacks; and addresses associated with ransomware payments, which are often associated with efforts to evade sanctions.

Internal controls – investigation

The third consideration is the evaluation process for potential sanctions violations. After the potential violations are identified through the screening process, manual investigation is required to determine whether there is a true match. If repeated alert closures due to non-matches are obvious during the manual review, these repetitive false matches should be incorporated into whitelists, to ensure that the names generating the false matches will not trigger alerts going forward. However, it is important to note that those whitelists should be reviewed each time changes are made to relevant sanctions lists. Relevant key controls within this area include: sufficient personnel to review sanctions alerts; policies and procedures specifying how alerts are adjudicated and the relevant information that must be included; and procedures for approval and communication of potential sanctions breaches to relevant authorities.

Auditing

Evaluating the auditing component of the sanctions compliance programme involves three key areas of focus with respect to screening. The first is determining if the configuration of automated screening tools is explicitly tied to the sanctions risk assessment. The second is performing an independent evaluation of the software configuration and results. This can be accomplished through an independent party that re-scans existing customers or transactions to determine if they receive similar results. Finally, it is important to determine how the company gains comfort over the outsourcing of any elements of the screening process. Where the entity relies on external parties to provide timely updated sanctions lists, or to screen against the lists and provide alerts, the company needs to confirm for itself whether or not those results match the configuration. As an example of where this can go wrong, in December 2021, TD Bank settled with OFAC for US$115,005 for violations of the North Korea and Drug Kingpin sanctions regimes. Within the North Korea violations, five employees at the North Korean Mission to the

United Nations were able to open accounts with North Korean passports because the bank relied on a vendor-supplied politically exposed persons list, which did not include government employees of sanctioned countries.[43]

Training

There are two key aspects to evaluating the training component of the sanctions compliance programme as it relates to screening. The first is determining if those charged with managing the sanctions screening process received specialised training that may include sanctions evasion techniques, data analytic methods related to fuzzy matching, and language or cultural training for understanding how names and punctuation differ between countries. The second is incorporating information learned during the potential sanctions match process into the sanctions training that is provided to the company widely. For example, after GE discovered the alleged sanctions violations noted above, during testing and auditing of its compliance programme, it implemented remedial measures, including developing a training video for employees using the violations as a case study.[44]

Sanctions screening in an investigation

A sanctions investigation can be initiated for a number of reasons, including an independent evaluation of a company's sanctions compliance programme, a tip from a whistle-blower, an adverse audit or compliance finding, or a regulatory inquiry. As part of any sanctions compliance investigation, the sanctions screening process and tools will require review. The investigation should include:

- review of the due diligence performed and included in the screening process;
- review of the specific data subject to screening and its field mapping;
- independent evaluation of the current screening configuration, such as fuzzy matching, in a test environment to see if it is comparable to what the screening tool is supposed to determine; and
- comparative analysis of search terms run through the existing screening tool against a sanctions search engine to determine if any likely matches were missed over time.

43 https://home.treasury.gov/system/files/126/20211223_TDBNA.pdf.

44 See footnote 28.

Conclusion

Complete and accurate sanctions screening is a critical component of any successful sanctions compliance programme. Many companies utilise automated sanctions screening tools to flag potential sanctions matches for further review. Regulators expect proper oversight and effective use of these sanctions screening programmes, which is evidenced in the recent settlement agreements for both financial and non-financial entities. While many entities focus on the capabilities of a sanctions screening programme, it is important to remember that a successful programme also requires proper oversight, a clear mapping between relevant sanctions risks for the entity and the sanctions screening configuration, and regular review to ensure results are complete, accurate and efficient.

APPENDIX 2

About the Authors

Charlie Steele
Forensic Risk Alliance

Charlie Steele is a partner in FRA's Washington, DC, office with more than 30 years of government and private-sector experience in civil and criminal compliance, investigations, enforcement and litigation matters, in a variety of industries and sectors. In recent years, he has specialised in economic sanctions and Bank Secrecy Act/anti-money laundering (BSA/AML) matters. He is a former senior US Treasury Department and Department of Justice official, serving most recently as chief counsel for the Office of Foreign Assets Control (OFAC). In that role, he led the team of lawyers providing legal advice and support to OFAC and other Treasury Department personnel in the formulation, implementation and enforcement of economic sanctions. Charlie has also served in a number of other senior positions in the Treasury Department: associate director for enforcement in OFAC, deputy director of the Financial Crimes Enforcement Network (FinCEN, the US government's principal BSA/AML agency, and the US Financial Intelligence Unit), and deputy chief counsel in the Office of the Comptroller of the Currency (the US supervisor and regulator of national banks). Charlie earned his JD from the Georgetown University Law Center and a BA in economics from the University of Virginia.

Gerben Schreurs
Forensic Risk Alliance

Gerben Schreurs is a partner in FRA's Zurich office and has over 25 years of experience solving technical challenges on complex problems requiring insight into large structured and unstructured data sets, including matters relating to investigations, risk management and compliance. He leads high-profile and confidential cases in the areas of money laundering, disputes, fraud, information leakage and regulatory breaches.

Prior to joining FRA, Gerben served as the global head of systems and controls for financial crime compliance at a major Swiss bank. Gerben managed a team of over 50 people internationally and was responsible for the operations and uplifts to compliance systems (transaction surveillance, name screening, sanctions and know-your-customer) with the aim to make processes more efficient and reduce regulatory risks by applying a consistent approach globally. Gerben qualified as a chartered EDP auditor in 2011 in the Netherlands.

Deborah Luskin
Forensic Risk Alliance

Deborah Luskin is an associate director in FRA's Washington, DC, office with over 19 years' experience in auditing and consulting. Deborah has experience in forensic accounting, financial audit attestation, risk management assessments, Sarbanes-Oxley 404 readiness and audit attestation and service organisation internal control assessments. While at FRA, Deborah has focused on regulatory reviews and anti-financial crime projects, including assisting companies in responding to regulatory inquiries, investigating potential non-compliance with anti-money laundering (AML) regulations, assessing AML and sanctions compliance programmes, developing risk assessments, drafting policies and procedures, and providing guidance regarding customer due diligence procedures. Prior to joining FRA, Deborah spent nine years at a Big Four firm working in risk management. Deborah specialised in assessing both financial and information systems internal controls supporting the financial statements, assessing regulatory compliance, performing fraud evaluations and assessing risk management programme effectiveness.

Deborah led large multinational teams in various industries. She is a certified public accountant, certified anti-money laundering specialist, certified global sanctions specialist, certified fraud examiner, certified information systems auditor certified cryptocurrency investigator and certified information systems security professional, as well as being certified in financial forensics.

Sarah Wrigley
Forensic Risk Alliance

Sarah Wrigley is a director based in FRA's London office. She has over 20 years' experience in complex, cross-jurisdictional investigations, including financial crime and sanctions, regulatory issues and accounting irregularities. She has worked across a range of industries, with a focus on financial services. Prior to joining FRA, Sarah was the Africa and Middle East regional head of financial crime intelligence and investigations for Standard Chartered Bank. Sarah led

the bank's investigation response in the region to global financial crime issues generating media and regulatory scrutiny. She led a team developing proactive intelligence on emerging financial crime themes covering money laundering and predicate offences, terrorist financing and potential sanctions breaches to identify and investigate higher risk clients.

Jona Boscolo Cappon
Forensic Risk Alliance

Jona Boscolo Cappon is a director based in FRA's London office. He has over 10 years' experience in applying data analytics, information technology and novel computational methods to solve complex business problems and drive data-informed decisions. He specialises in delivering analytics-driven solutions to global financial and non-financial institutions to help them respond to business-critical events by identifying, quantifying and mitigating risks. Jona has led forensic technology teams to design fraud detection analysis, develop monitoring capabilities and support clients across the public, corporate and financial sectors to respond to global regulators. He has experience in leading forensic investigations and complex regulatory compliance projects covering issues relating to fraud, bribery, anti-money laundering, sanctions violations, customer contract breaches and other complex financial crimes. While at FRA, Jona has focused on network analytics, graph databases and natural language processing techniques to automate the analysis and linking of a variety of data sets and uncover entities with sophisticated organisational structures involved in money laundering. Prior to joining FRA, Jona spent six years in the forensic technology team of a Big Four firm, where he led teams with disparate backgrounds to investigate regulatory breaches through the development of tailor-made software and interactive visualisations.

Forensic Risk Alliance
Bahnhofstrasse 100
Zurich 8001
Switzerland
Tel: +41 795 002 991
gschreurs@forensicrisk.com

Audrey House
16–20 Ely Place
London EC1N 6SN

United Kingdom
Tel: +44 20 7831 9110
swrigley@forensicrisk.com
jcappon@forensicrisk.com

2550 M Street NW
Washington, DC 20037
United States
Tel:+1 202 627 6580
csteele@forensicrisk.com
dluskin@forensicrisk.com

www.forensicrisk.com

We live in a new era for sanctions, more than ever, it seems. More states are using them, in more creative (and often unilateral) ways. They've become many states' first line of response.

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

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

ISBN 978-1-83862-874-1