Global Investigations Review

The Guide to Sanctions

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

Second Edition

The Guide to Sanctions

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

Editors

Rachel Barnes

Paul Feldberg

Nicholas Turner

Anna Bradshaw

David Mortlock

Anahita Thoms

Rachel Alpert

GIR
Global Investigations Review

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

www.globalinvestigationsreview.com

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

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

ISBN 978-1-83862-596-2

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

Acknowledgements

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

BAKER & HOSTETLER LLP

BAKER MCKENZIE

BARNES & THORNBURG LLP

BDO USA LLP

CARTER-RUCK SOLICITORS

CRAVATH, SWAINE & MOORE LLP

EVERSHEDS SUTHERLAND

FORENSIC RISK ALLIANCE

GLOBAL LAW OFFICE

JENNER & BLOCK LLP

MCGUIREWOODS LLP

MAYER BROWN

MILLER & CHEVALIER CHARTERED

PETERS & PETERS SOLICITORS LLP

SEWARD & KISSEL

SIMMONS & SIMMONS LLP

STEPTOE & JOHNSON

STEWARTS

THREE RAYMOND BUILDINGS

WHITE & CASE LLP

WILLKIE FARR & GALLAGHER LLP

Publisher's Note

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

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

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

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

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

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

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

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

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

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

David Samuels
Publisher, GIR
June 2021

Contents

Foreword

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

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

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

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

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

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

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

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

Part II

Compliance Programmes

14

Sanctions Screening: Challenges and Control Considerations

Charlie Steele, 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 (also known as 'smart' 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 by sanctioned parties, under OFAC's 50 Percent Rule.

A more recent 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 persons, companies and entities in specified sectors of the Russian economy (especially energy, finance and armaments), prohibiting certain types of activity by US persons with individuals or entities operating in those sectors. 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 types of activities in which the targets were engaged.

---

1 Charlie Steele is a partner, Sarah Wrigley is a director and Deborah Luskin and Jona Boscolo Cappon are associate directors 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.

Sanctions screening failures have figured prominently in a number of OFAC penalty settlements, with both financial and non-financial entities. To this end, we will review 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. Within the US Department of the Treasury's 2019 'A Framework for OFAC Compliance Commitments' (the 'Framework'),[4] after addressing five high-level elements for a sound sanctions compliance programme, it 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.[5] 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 violations, but there are several more that we will discuss throughout this chapter.

In 2015, OFAC published a one-page guidance document regarding the management of 'false hits' lists.[6] 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. NYDFS had 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, NYDFS set out specific requirements for these programmes[7] that require Boards of Directors or Senior Officers to certify compliance on an annual basis.[8]

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

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

5 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, organisations have failed to update their sanctions screening software to incorporate updates to the SDN List or SSI 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 utilise such alternative spellings (i.e., Habana instead of Havana, Kuba instead of Cuba, Soudan instead of Sudan, etc.).

6 https://home.treasury.gov/system/files/126/false_hit.pdf.

7 Part 504 of the New York State Banking Regulations in 2017.

8 www.dfs.ny.gov/industry_guidance/transaction_monitoring.

- *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.*

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:

- *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.*

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*

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

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.[9] 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.*

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 their 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 published 'Guidance on Sanctions Screening' in 2019.[10] The guidance indicates that sanctions screening should be supported by key enabling functions, such as policies 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 (SCP)

Sanctions screening does not operate in a vacuum; it is an integrated piece of the sanctions compliance programme. In this section, we will describe some of the key elements of an

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

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

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 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, 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, tested to ensure they provide results in accordance with the identified risks, and 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 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, proper 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. 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 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.

- February 2021: BitPay, Inc., a digital currency business, settled with OFAC for US$507,375 for processing payments for over five years, where they possessed Internet Protocol (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 purposes.[11] BitPay, Inc. screened the merchants, but not the end customers, against relevant sanctions lists, even though they were in receipt of end-customer information. 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.[12]
- December 2020: National Commercial Bank settled with OFAC for US$653,347 for processing payments to sanctioned entities.[13] One of the mitigating factors in determining the penalty included the future 'required screening of all payments against international sanctions lists'.
- September 2020: Deutsche Bank Trust Company Americas settled with OFAC for US$583,100 for processing Ukraine-related payments.[14] There were several issues with their screening software, but one in particular is that they did not include the SWIFT Business Identifier Code (BIC) in their sanctions screening, which allowed payments to be made to a designated financial institution.
- June 2019: Western Union settled with OFAC for US$401,697 because a bank in The Gambia, serving as one of their principal master agents, used a sub-agent that was on a sanctions list.[15] Western Union had erroneously recorded the sub-agent as a location of the master agent, rather than as a distinct legal entity. There was a process to screen master agents and sub-agents, but they did not screen the location data for the sub-agents. Because Western Union mistakenly believed that the Gambia-based company had operated out of a single location that had been closed, the sub-agent continued to serve as sub-agent for another month.
- April 2019: Standard Chartered Bank settled with OFAC for US$639,023,750 for several sanctions violations, including online and mobile banking platforms that, for many years, did not include comprehensive sanctions screening.[16]

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.

11 https://home.treasury.gov/system/files/126/20210218_bp.pdf.
12 https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
13 https://home.treasury.gov/system/files/126/20201228_NCB.pdf.
14 https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
15 https://home.treasury.gov/system/files/126/20190607_western_union.pdf.
16 https://home.treasury.gov/system/files/126/scb_settlement.pdf.

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

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 if 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, airplanes 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 Arabic names in Roman script introduces at least a dozen name variations for the former Libyan leader Gaddafi, ranging from Qaddafi to Elkaddafi.

'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 fuzzing 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 datasets 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 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:

- 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.[17]
- 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.[18] In another example, Amazon 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.[19] 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: The General Electric Company settled with OFAC for US$2,718,581 for accepting payments from an entity on the SDN List.[20] The 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 the GE Companies' sanctions screening software, which screened only the abbreviation of the SDN's name, never generated an alert on Cobalt's name.
- November 2018: Cobham Holdings, Inc. settled with OFAC for US$87,507 for screening software that failed to generate an alert against JSC AlmazAntey (as identified on the SDN List) for payments made to Almaz Antey Telecommunications LLC.[21] The third-party screening software relied on by Cobham used an 'all word' match criteria that would only return matches containing all of the searched words, even though Cobham had set the search criteria to 'fuzzy' to detect partial matches. This meant that the software failed to match 'Almaz Antey' when Cobham searched for 'Almaz Antey Telecom.' Almaz-Antey Telecommunications LLC was 51 per cent owned by the SDN.
- October 2018: OFAC issued a Finding of Violation to JPMorgan Chase Bank – formally determining that the bank had committed violations, but declining to impose a monetary penalty – because the bank's screening software did not identify SDN-listed persons.[22] From 2007 to October 2013, they used a vendor screening system that failed to identify customers with potential matches to the SDN List. The system's screening logic capabilities failed to identify customer names with hyphens, initials, or additional middle or last names as potential names. After transitioning to a new system in 2013, JPMC re-screened

17 https://home.treasury.gov/system/files/126/20200909_DBTCA.pdf.
18 https://home.treasury.gov/system/files/126/20200708_amazon.pdf.
19 https://home.treasury.gov/system/files/126/20191125_apple.pdf.
20 https://home.treasury.gov/system/files/126/20191001_ge.pdf.
21 https://home.treasury.gov/system/files/126/20181127_metelics.pdf.
22 https://home.treasury.gov/system/files/126/jpmc_10050218.pdf.

188 million clients' records through the new system and reported the historical violations to OFAC.

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:

- BitPay, Inc.'s February 2021 settlement with OFAC noted that the company's changes to its compliance programme included blocking of IP addresses that appear to originate in sanctioned jurisdictions, including end-customer information in the screening process, and launching a new customer identification tool for merchant's buyers.[23]
- In a January 2021 settlement with OFAC, PT Bukit Muria Jaya procured sanctions screening services from a third-party provider.[24]
- In a January 2021 settlement, OFAC noted that Union de Banques Arabes et Francaises now utilises the sanctions screening software used by their largest shareholder, which includes screening the client database, an anti-stripping module, negative news research, risk database research, vessel screening and country screening.[25]
- 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 screening configuration criteria on a periodic basis, screening all 'hot wallets[26]' against the SDN List, including cryptocurrency wallet addresses identified by OFAC, and a retroactive batch screen of all users.[27]
- In a December 2020 settlement, OFAC noted that National Commercial Bank now requires screening of all payments against international sanctions lists, and requires sanctions checks during account openings.[28]
- Amazon.com Inc.'s July 2020 settlement with OFAC notes several improvements to the company's screening processes, including employment of internal and third-party sources to conduct thorough reviews of Amazon's automated screening systems to address screening failures, incorporation of additional automated preventative screening controls, development of internal custom screening lists to minimise the risk of processing transactions that raise sanctions compliance concerns, and enhancement of its sanctioned jurisdiction IP blocking controls and implementation of automated processes to continually update its mapping of IP ranges associated with sanctioned jurisdictions.[29]

23 https://home.treasury.gov/system/files/126/20210218_bp.pdf.
24 https://home.treasury.gov/system/files/126/20210114_BMJ.pdf.
25 https://home.treasury.gov/system/files/126/01042021_UBAF.pdf.
26 Cryptocurrency wallet that is online and connected in some way to the internet.
27 https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
28 https://home.treasury.gov/system/files/126/20201228_NCB.pdf.
29 https://home.treasury.gov/system/files/126/20200708_amazon.pdf.

- In its February 2020 OFAC settlement, Societe Internationale de Telecommunications Aeronautiques SCRL implemented extensive remedial efforts and enhancements to its customer and supplier screening.[30]
- In its June 2019 settlement with OFAC, Hotelbeds USA implemented an enhanced third-party IT solution with a sanctions screening tool.[31]

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.[32] 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.[33] The invoices were not paid within that time frame and this violated Directive 2 under the Russia sectoral sanctions, which 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.[34]

Another example is the recent ban on US-person investment in Communist Chinese Military Companies (CCMCs) 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 44 specified CCMCs?).[35] 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 if potential sanctions violations have occurred.

OFAC's 50 Percent Rule adds an additional element to screening complexity. Under this rule, the property and interests in property of an entity are blocked if the entity is owned, directly or indirectly, 50 per cent or more by one or more persons whose property and interests in property are blocked.[36] 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 Wolfsberg Group's sanctions screening guidance contains a discussion regarding the assessment of which data elements to screen.[37] 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*

30 https://home.treasury.gov/system/files/126/20200226_sita.pdf.
31 https://home.treasury.gov/system/files/126/20190612_hotelbeds_0_1.pdf.
32 https://home.treasury.gov/system/files/126/ukraine_eo3.pdf.
33 https://home.treasury.gov/system/files/126/20190425_haverly.pdf.
34 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/876971/200331_-_SCB_Penalty_Report.pdf.
35 https://home.treasury.gov/system/files/126/13959.pdf.
36 https://home.treasury.gov/system/files/126/licensing_guidance.pdf.
37 https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%20Guidance%20on%20Sanctions%20Screening.pdf.

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 – 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. One 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.

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, GE implemented remedial measures, including developing a training video for employees using the violations as a case study.[38]

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 match, 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.

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.

38 See footnote 20, above.

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 FIU), 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.

Sarah Wrigley
Forensic Risk Alliance

Sarah Wrigley is a director based in FRA's London office. She has over 18 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. Sarah previously spent 11 years in the forensic accounting team of a Big Four firm, and has led investigations into corporate and procurement fraud, embezzlement, regulatory breaches, accounting misstatements and bribery and corruption. Sarah is a UK-qualified chartered accountant, a certified fraud examiner and a certified anti-money laundering specialist.

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 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. Deborah is a certified public accountant, certified anti-money laundering specialist, certified global sanctions specialist, certified fraud examiner, certified in financial forensics, certified information systems auditor and certified information systems security professional.

Jona Boscolo Cappon
Forensic Risk Alliance

Jona Boscolo Cappon is an associate 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 datasets 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
Audrey House
16–20 Ely Place
London EC1N 6SN
United Kingdom
Tel: +44 20 7831 9110
swrigley@forensicrisk.com
jboscolocappon@forensicrisk.com

550 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 states are using them, in more creative (and often unilateral) ways.

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

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

an LBR business

ISBN 978-1-83862-596-2