THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

Bulletin

of The International Academy of Financial Crime Litigators

ISSUE 2 | FALL 2023

Bulletin of The International Academy of Financial Crime Litigators

Paris, France

Editor: Jonathan S. Sack

Editorial Board/Publishers: Stéphane Bonifassi, Lincoln Caylor and Elizabeth Ortega

Publication/Art Director: ECO Strategic Communications

The Bulletin appears twice a year and is available free of charge.

Current and back issues are available online at:
https://financialcrimelitigators.org/publications/

To sign up for a subscription or to report an address change please send an email to contact@financialcrimelitigators.org.

For editorial comments or inquiries, please contact the editor at jsack@maglaw.com or at the address below.

For further information about The Academy, please visit our website www.financialcrimelitigators.org.

For general inquiries, please send an email to contact@financialcrimelitigators.org.

ISSN 2999-3938

Contents

ISSUE 2 | FALL 2023

Letter FROM THE EDITOR

Welcome to the second issue of the Bulletin of the International Academy of Financial Crime Litigators. The Academy's mission is to join theory and practice, and this issue of the Bulletin fulfills that dual mission in exemplary fashion. Our authors cover a wide range of topics, demonstrating the great depth and breadth of expertise among Academy Fellows and their colleagues.

We begin with an article by **Daniel Pascucci*** and **Michael Godwin** about a recent U.S. Supreme Court decision, *Yegiazaryan v. Smagin*, and its implications for using the Civil RICO law as a means to recover assets in the United States. Dan and Michael place the decision in the context of broader efforts to recover assets for victims and thoughtfully consider what they call "the daunting burdens" of making effective use of a federal civil RICO cause of action.

Next, **Wendy Lin*** and **Leow Jiamin** serve as expert guides through the thicket of crypto-related fraud and disputes. They explain, among other things, how disclosure orders can help identify and recover assets from unknown participants in illegal schemes, and how freeze orders can preserve the status quo while claims are being litigated. Wendy and Leow shed light on the intersection between asset recovery and the rapidly changing world of crypto assets.

Jitka Logesova* and **Jaromir Pumr** enlighten us on the increasing importance of regulatory due diligence prior to completing corporate merger and acquisition transactions. Jitka and Jaromir astutely observe that due diligence has often been thought of in narrow financial or reputational terms, which typically ignores compliance and regulatory risks that may be substantial but not obvious or discernible without careful examination. Their article is particularly timely in light of the recent announcement by the U.S. Department of Justice that acquirers which identify and disclose violations in a timely way may be eligible for leniency.

Kateryna Boguslavska of the Basel Institute on Governance updates us on the Institute's Anti-Money Laundering Index results for 2023. As Kateryna explains, the findings are "rather depressing," with the risk of money-laundering, terror finance and related offenses on the rise based on the AML Index's detailed risk assessment. The article helpfully focuses our attention on three areas of potential improvement: freezing and confiscating illicit funds, regulating crypto assets, and addressing misuse of not-for-profit entities.

Lastly, **Maria Nizzero*** gives us a highly informative update on recent litigation over sanctions imposed in the United Kingdom. Since Russia's invasion of Ukraine in February 2022, governments have used sanctions to wield white-collar regulatory and enforcement efforts in furtherance of national security goals. This has played out in the United States, where DOJ officials have started calling sanctions the "new FCPA," and in the United Kingdom, where the targets of sanctions have challenged regulatory action in the courts, as Maria explains. Maria provides insight on how courts have ruled on such challenges to date and what issues are still to be clarified.

In sum, this issue of the Bulletin reflects the Academy's wide-ranging interest in all aspects of financial crimes: a plaintiff's vigorous efforts to recover assets after being victimized by fraud; a defendant's vigorous efforts to defend against regulatory and criminal enforcement; and governmental and non-governmental authorities' interest in adherence to law. We hope you find this rich material of interest.

**** Fellows of The Academy***

I hope you enjoy
this issue of
The Academy Bulletin.

Jonathan S. Sack* | *Editor*

The Thermonuclear Option:

Civil RICO as an Asset Recovery Tool in U. S. Enforcement Efforts post-*Smagin*

DANIEL PASCUCCI

MICHAEL GODWIN

Introduction

In recent years, the United States has received heightened attention as a haven for asset secrecy and inventive wealth-protection devices – and, consequently, a forum for asset-recovery litigation. The Supreme Court recently weighed in on the fight against fraudulent judgment-evasion schemes when it held that foreign plaintiffs with arbitration awards enforceable in the United States may have standing to assert civil RICO claims to enforce those awards. *See Yegiazaryan v. Smagin,* 143 S. Ct. 1900 (2023) (*"Smagin"*).

Civil RICO, labeled by one circuit court "the litigation equivalent of a thermonuclear device," packs a powerful punch – combining considerable stigma, the threat of high litigation costs and potential liability for treble damages and attorneys' fees. *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991). Coupled with robust discovery rights attendant to federal court litigation, RICO can be a powerful and effective tool in a U.S. asset-recovery campaign.

While *Smagin* clarified standing to assert RICO claims, it did not modify the daunting burdens a plaintiff must clear to prevail on such claims. Most private RICO claims fail. *See Gross v. Waywell,* 628 F. Supp. 2d 475, 480 (S.D.N.Y. 2009) (surveying four years of civil RICO cases and determining "all resulted in judgments against the plaintiffs," with none even surviving to trial). The *Gross* court described civil RICO as a "siren's song," drawing "spellbound plaintiffs foundering against the rocks." *Id.* at 479.

Smagin may have amplified the siren's call around the world, but the rocks remain. This article seeks to shed light on the rocks and RICO's potential role in piercing complex schemes to evade enforcement. We are only aware of one case in which a foreign plaintiff successfully used RICO to enforce an arbitration award and reach trial, *Tatung v. Shu Tze Hsu*, 217 F. Supp. 3d 1138 (C.D. Cal. 2016) (on which one of the authors served as lead plaintiff's counsel), and that was only after surviving 35 motions to dismiss and summary judgment motions. We draw on our experience successfully navigating that case to highlight the unique complexities of using RICO as an asset-recovery tool and factors creditors should consider when assessing whether theirs is the rare case in which the advantages of this nuclear option outweigh the pitfalls.

THE WILD WEST AND THE NEED FOR SHARPER TOOLS TO PIERCE U.S. MONEY LAUNDERING AND WEALTH-DEFENSE SCHEMES

The past few years have illuminated the United States as a preeminent destination for wealth-defense and asset-protection strategies. The 2021 Pandora Papers exposed how billionaires utilize extreme financial secrecy laws of western states like South Dakota, Alaska, Nevada and Wyoming to move assets off their balance sheets while maintaining the privileges of ownership. A Bloomberg review of state records tallied deposits of a *half-trillion dollars* just in trusts created under South Dakota's privacy-driven laws. *See* Anders Melin, *The World's Rich And Powerful Are Stashing $500 Billion In This Tax Haven,* FINANCIAL ADVISOR MAGAZINE (Oct. 14, 2021), https://www.fa-mag.com/news/the-world-s-rich-and-powerful-are-stashing--500-billion-in-this-tax-haven-64394.html?section=3. And, as of 2023, the Tax Justice Network now ranks the United States as number one in its Financial Secrecy Index. *See Financial Secrecy Index 2022,* TAX JUSTICE NETWORK, https://fsi.taxjustice.net. With the sheer volume of hidden and open wealth flowing through the United States, there has never been a greater need for sharp tools to enforce creditor rights against debtors willing to go to great lengths to avoid collection.

American asset-recovery practitioners already have a well-honed arsenal of tools for investigations and enforcement litigation. In addition to far-reaching long-arm jurisdiction, the United States has uniquely expanded the scope of discovery. *See, e.g. In re Ishihara Chem. Co.,* 121 F. Supp. 2d 209, 225 (E.D.N.Y. 2000) ("[T]he U.S. system of broad discovery is fundamentally different from that of most foreign countries . . . most other countries fiercely limit the scope of discovery to protect personal privacy and consider U.S. discovery to be a fishing expedition.") (citation and quotation omitted). The opportunity to add RICO claims to the mix is compelling. RICO puts at issue a broad array of facts, often delving deeply into the internal affairs and relationships among all the players in an alleged RICO enterprise. *See, e.g., Black v. Ganieva,* 619 F. Supp. 3d 309, 334 (S.D.N.Y. 2022). Discovery in a civil RICO case will often lead to a deep understanding of how – *and where* – a defendant moves assets. Along with its mandatory treble damages and fee-shifting provisions, the potential availability of RICO in asset-recovery litigation is alluring.

THE SIREN'S SONG: THE U.S. SUPREME COURT CONFIRMS WHEN FOREIGN PLAINTIFFS CAN ASSERT CIVIL RICO CLAIMS TO ENFORCE NON-U.S. ARBITRATION AWARDS

The Supreme Court's decision in *Smagin* resolved a split among lower courts over whether foreign creditors have standing to assert a civil RICO claim to enforce arbitration awards and judgments. The discord stemmed from *RJR Nabisco, Inc. v. European Cmty.,* 136 S. Ct. 2090 (2016), where the Court considered whether RICO applies extraterritorially. Concerned that allowing extraterritorial reach of private claims could put the statute in conflict with laws of other countries providing redress for such injuries, the Court held that civil RICO "does not allow recovery for foreign injuries," and a private RICO plaintiff must "allege and prove a *domestic injury* to business or property." *RJR Nabisco,* 136 S. Ct. at 2096, 2111 (emphasis added). Unfortunately, *RJR Nabisco* provided little guidance on how to identify or define a domestic injury, and a split among lower courts ensued.

District courts in California and New York promptly adopted competing schools of thought. In *Bascuñan v. Elsaca,* 2016 WL 5475998 (S.D.N.Y. Sept. 28, 2016), the Southern District of New York applied RJR Nabisco to section 1964(c) claims by a Chilean citizen and resident. Noting that a partial dissent by Justice Ginsberg posited that the majority decision in RJR Nabisco makes a "RICO private cause of action 'available to domestic but not foreign plaintiffs,'" the court held that a plaintiff feels the effects of a financial injury in the place of its residence, and therefore the plaintiff had not suffered a domestic injury addressable by RICO's private right of action. Id. at 5-6 (citation omitted).

Just weeks later, in *Tatung v. Shu Tze Hsu,* 217 F. Supp. 3d 1138 (C.D. Cal. 2016), the Central District of California reviewed *RJR Nabisco* and the nascent *Bascuñan* decision in a case by a Taiwanese plaintiff seeking to enforce an arbitration award against an alleged global RICO enterprise used to siphon assets of a California debtor to related offshore parties. The court found the *Bascuñan* effects test would "amount[] to immunity for U.S. corporations who, acting entirely in the United States, violate civil RICO at the expense of foreign corporations doing business in this country." *Id.* at 1155. Instead, the court focused on where the defendants' conduct was directed and

recognized that, armed with an arbitration award and judgment enforceable in California, the plaintiff had domestic enforcement rights, which the defendants specifically targeted. *Id.* at 1157.

This split between assessing where the effects of racketeering activity are felt and assessing where the activity is targeted quickly expanded to the circuit courts. The Seventh Circuit embraced the New York approach and "adopted a rigid, residency-based test for domestic injuries involving intangible property, such as a judgment," which "locates an injury to intangible property at the plaintiff's residence." *Smagin,* 143 S. Ct. at 1907 (citing *Armada (Sing.)* PTE *Ltd. v. Amcol Int'l Corp.,* 885 F. 3d 1090 (2018)). Meanwhile, *Bascuñan* made its way through two appeals, and the Second Circuit ultimately reversed, holding a foreign plaintiff may allege a domestic injury where the injury is to property the plaintiff maintains in the United States, but limited its holding to tangible property. *Bascuñan v. Elsaca,* 874 F.3d 806, 814 (2d Cir. 2017).

The Third Circuit also rejected the Seventh Circuit's effects test and instead adopted a context and case-specific analysis. *See Humphrey v. GlaxoSmithKline PLC*, 905 F.3d 694, 709 (3d Cir. 2018). In rejecting the Seventh Circuit's bright-line rule, the Third Circuit held that when assessing whether alleged injuries are domestic or foreign, courts "must engage in a fact-intensive inquiry that will ordinarily include consideration of multiple factors that vary from case to case," and which are not limited to the location of the plaintiff's residence. *Id.* at 701, 707.

Post-*GlaxoSmithKline*, the *Smagin* case reached the Ninth Circuit. *Smagin v. Yegiazarian*, 37 F. 4th 562, 567-68 (9th Cir. 2022). Smagin, a resident and citizen of Russia, had won an $84 million arbitral award in London against Yegiazaryan for fraudulent misappropriation in a real estate venture in Moscow. To avoid a Russian criminal indictment, Yegiazaryan fled to California. Smagin obtained a judgment in California recognizing the London award and brought a civil RICO action alleging an extensive pattern of racketeering activity to hide assets and frustrate enforcement of the California judgment.

The Ninth Circuit declined to follow the Seventh Circuit's residency-based approach, instead adopting a context-specific inquiry consistent with the Third Circuit in *GlaxoSmithKline*. *See id.* (some citations omitted). The Ninth Circuit concluded that Smagin sufficiently pleaded a domestic injury "because he had alleged that his efforts to execute on a California judgment

in California against a California resident were foiled by a pattern of racketeering activity that largely 'occurred in, or was targeted at, California' and was 'designed to subvert' enforcement of the judgment in California." *Smagin*, 143 S. Ct. at 1907 (citing *Smagin*, 37 F. 4th at 567-68 (9th Cir. 2022)).

The Supreme Court affirmed the Ninth Circuit's context-specific inquiry, holding that "determining whether a plaintiff has alleged a domestic injury [for purposes of RICO] is a context-specific inquiry that turns largely on the particular facts alleged in a complaint." *Id*. at 1909 (citation omitted). Under that approach, Smagin's allegations that his "interests in his California judgment against Yegiazaryan, a California resident, were directly injured by racketeering activity either taken in California or directed from California, with the aim and effect of subverting Smagin's rights to execute on [his] judgment in California . . . suffice to state a domestic injury." *Id*.

ROCKS IN THE WATER: NAVIGATING THE DAUNTING BURDENS OF CIVIL RICO TO ENFORCE FOREIGN ARBITRATION AWARDS

Smagin marks an important development in RICO jurisprudence – clarifying where a RICO injury is measured and opening the door to foreign plaintiffs to use this sharp tool to enforce awards and judgments they patriate to the United States. But domestic injury is just one of many requirements to state a private RICO claim and there are many reasons why, as the Southern District of New York observed, most such claims are doomed from the start. The pleading and proof requirements are exacting and beyond the reach of all but the most extreme cases. While courts have labored for decades to define the precise burdens a civil RICO plaintiff faces – even differing over the number of elements to be proven – the Second Circuit Court of Appeals recently provided a succinct statement likely to be cited frequently:

> For a RICO claim to survive, a plaintiff must adequately allege "the existence of seven constituent elements: (1) that the defendant[s] (2) through the commission of two or more acts (3) constituting a 'pattern'(4) of 'racketeering activity'(5) directly or indirectly invests in, or maintains an interest in, or participates in (6) an 'enterprise'(7) the activities of which affect interstate or foreign commerce."

MinedMap, Inc. v. Northway, 2022 U.S. App. LEXIS 5098, at *2 (2d Cir. Feb. 25, 2022) (citations omitted). Unpacking the burdens of each of these elements is beyond the aim of this article, but employing several best practices to evaluate claims before asserting RICO can help avoid the most common pitfalls.

The Single Operator Problem

Plaintiffs considering a civil RICO charge should carefully assess the nature and operation of the target defendant(s). RICO can be a tempting weapon in enforcement cases involving a heavy-handed operator of a debtor company, particularly where the owner/operator has deep pockets but has fleeced the debtor into insolvency. In such circumstances, however, without additional evidence of a broader enterprise, a valid RICO claim rarely lies and alter ego or fraudulent conveyance claims would be better suited to unwind the fleecing. RICO imposes a strict requirement to plead and prove a clear dichotomy between the defendant(s) and the enterprise. Courts consistently reject "the idea that a RICO enterprise may consist 'merely of a corporate defendant associated with its own employees or agents carrying on the regular affairs of the defendant.'" *Cruz v. FXDirectDealer, LLC,* 720 F.3d 115, 121 (2d Cir. 2013) (citations omitted). RICO claims should be reserved for instances where there is a clear "enterprise" distinct from the target defendants, through which the defendants operated.

The Problem with Mail Fraud and Wire Fraud

Before deciding to proceed with a RICO claim, Plaintiffs should carefully consider whether they have the evidence to plead and prove numerous predicate acts other than or in addition to mail fraud or wire fraud. 18 U.S.C. § 1961(1) enumerates a long list of potential predicate acts. The most common crimes alleged in civil cases, mail fraud and wire fraud, will invoke automatic elevated suspicion because of the risk that even ordinary business activity can be painted as fraudulent and conducted by mail or electronic means. As the Second Circuit described in *MinedMap*, "RICO claims premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." 2022 U.S. App. LEXIS at *2.

Some courts have taken this scrutiny further, creating an enhanced continuity requirement for cases invoking mail or wire fraud. *See, e.g., Feinstein v. Resolution Trust Corp.*, 942 F.2d 34, 46 (1st Cir. 1991) ("We hold

that, in assessing the longevity of a RICO scheme involving allegations of mail fraud, the scheme's duration must be measured by reference to the particular defendant's fraudulent activity, rather than by otherwise innocuous or routine mailings that may continue for a long period of time thereafter."). This requirement has been applied to require a plaintiff to establish a pattern and continuity with reference only to those communications independently comprising fraud, disregarding correspondence that may be part of an alleged scheme but are not independently fraudulent. *See, e.g., In re Am. Exp. Co. S'holder Litig.*, 840 F. Supp. 260, 264 (S.D.N.Y. 1993).

The Rule 9 Challenge

A plaintiff considering filing a RICO claim in the first litigation against a target defendant would be well advised to consider whether antecedent claims would better set up a proper assessment and assertion of RICO. In most civil RICO cases, the racketeering activity will sound in fraud, invoking the particularity requirement of Federal Rule of Civil Procedure 9(b), meaning allegations of predicate acts, pattern and continuity must be detailed with particularity. *See, e.g. Feinstein,* 942 F.2d at 42 ("It is settled law in this circuit that Fed.R.Civ.P. 9(b), which requires a party to plead fraud with particularity, extends to pleading predicate acts of mail and wire fraud under RICO.").

Meeting these requirements demands a more extensive level of pre-suit investigation and preparation than most other claims available to a plaintiff contemplating a civil RICO claim. In practice, asset recovery campaigns often require filing more than one case and the litigation leading to the underlying award or judgment can be a vital source of information to support the specificity required to conform to Rule 9 in the RICO context. This bar cannot be met with general allegations and averments on information and belief, but instead requires detailed knowledge about the enterprise and predicate acts that is often beyond the reach of investigation tools. In *Tatung*, we filed RICO claims only after several prior hard-fought cases yielded sufficient discovery to allege a highly-detailed description of the enterprise and its operations. Without the valuable discovery obtained in the antecedent cases, it is unlikely the case would have survived pre-trial motions, let alone provide the leverage to settle successfully during trial.

A New Sequencing Challenge

For foreign plaintiffs, the new path *Smagin* forged will likely prove narrow. To allege domestic injury, the plaintiff must plead – with specificity in most cases – that the pattern of racketeering was directed at and impacted U.S. enforcement rights. To meet this burden, the pattern will likely need to post-date a U.S. judgment recognizing and enforcing the award or foreign judgment or meaningfully continue after such a judgment is entered. This two-step process may require that a plaintiff holding a foreign judgment or award first patriate it to a U.S. judgment, then seek to enforce it under conventional post-judgment creditor rights. If those efforts are thwarted by a post-judgment pattern of racketeering, *Smagin* provides a path to civil RICO standing.

CONCLUSION

As the *Gross* survey of cases demonstrated, most civil RICO cases will not survive pre-trial motions, resulting instead in higher expenses and poorer outcomes than more readily established common law claims on the same facts. *See Gross*, 628 F. Supp. 2d at 480. For a creditor seeking to enforce a judgment or award against what appears on its face to be a RICO enterprise, successful and cost-effective enforcement requires diligence at the outset to decide whether asserting a civil RICO claim is likely to yield a better outcome or just drive up expenses. While such claims should be brought judiciously, in the right case, the reach and impact of electing the thermonuclear option can provide a much-needed sharp tool to pierce the most elaborate asset-protection schemes.

AUTHORS

Daniel Pascucci

Fellow Daniel Pascucci is a member in Mintz's litigation section and is Co-Chair of the firm's Cross-Border Asset Recovery practice and Managing Member of the San Diego office.

Michael Godwin

Michael Godwin is an associate in Mintz's litigation section in San Diego. His practice focuses on Cross-Border Asset Recovery and complex commercial litigation.

Share This Read

Legal Tools

Available To Claimants Seeking To Recover Assets In Crypto-Related Disputes

WENDY LIN

LEOW JIAMIN

Introduction

Crypto-related fraud shows no signs of slowing down. The media have reported that crypto crime hit a record US $20 billion in 2022; cryptocurrency investment fraud tripled from 2021 to 2022; and losses to crypto fraud in the UK increased more than 40% from March 2022 to 2023.

Waves of insolvency have also hit the crypto industry, including the bankruptcy of FTX Trading Ltd, and cryptocurrency lender Celsius Network LLC. Litigation has been commenced by the United States Securities and Exchange Commission against various cryptocurrency exchanges.

It is therefore unsurprising that we have seen more instances of courts (in Singapore and other jurisdictions) tackling legal issues relating to cryptoassets and granting novel orders to keep up with the growing needs of crypto-related disputes.

We summarize some of these recent developments, focusing on the legal tools and options available to claimants seeking to recover cryptoassets in such fraud and disputes, including:

a. How can disclosure orders be served out of jurisdiction to seek information in respect of unknown fraudsters;

b. How freezing orders can be sought in a novel form in respect of cryptoassets;

c. How recovery of cryptoassets can be sought against crypto exchanges; and

d. How recovery of cryptoassets can be sought against blockchain developers.

SERVING DISCLOSURE ORDERS OUT OF JURISDICTION: SEEKING INFORMATION ABOUT UNKNOWN THIRD-PARTIES

The defendant in crypto fraud disputes is often unknown. A claimant would typically attempt to seek information from crypto exchanges to identify these

fraudsters. Disclosure orders can be sought: (a) in support of injunctions (such as freezing or interim injunctions); (b) against non-parties to request documents to assist with a tracing claim where there is a *prima facie* case of fraud (*ie*, "*Bankers Trust* orders"); or (c) against non-parties who have become "mixed-up" in wrongdoing to provide information (*i.e.* "*Norwich Pharmacal* orders").

More often than not, the crypto exchanges would not be located in the same jurisdiction as the claimant. These crypto exchanges may also utilise opaque structures with numerous corporate entities situated across multiple jurisdictions, making it difficult for claimants to know which precise crypto exchange entity is involved or would hold useful information.

Traditionally, the UK Courts have found that it is more likely than not that a *Bankers Trust* order can be served against a party outside the jurisdiction "*in exceptional circumstances … includ*[ing] *cases of hot pursuit*" (*Ion Science Limited and or v Persons Unknown and ors No. CL-2020-000840* at [21]), but have not permitted *Norwich Pharmacal* orders to be served out of jurisdiction. To address this, the Practice Direction 6B of the UK Civil Procedure Rules 1998 had from 1 October 2022 included a new paragraph 3.1(25) to allow service of orders seeking information "regarding *(i) the true identity of a defendant or a potential defendant and/or (ii) what has become of the property of a claimant or applicant*" for commencement of proceedings in the UK.

In *LMN v Bitflyer Holdings Inc and ors* [2022] EWHC 2954 (Comm) ("*LMN*"), the English High Court thus permitted the orders to be served out of jurisdiction under paragraph 3.1(25). The English High Court explained that it "*would be impractical and contrary to the interests of justice to require a victim of fraud to make speculative applications in different jurisdictions to seek to locate the relevant exchange company and then to seek disclosure, probably in aid of foreign proceedings*". Instead, any concerns about national laws can be dealt with by ordering that no respondent is required to do anything contrary to local laws (*LMN* at [35]-[37]).

In Singapore, the Rules of Court 2021 that came into operation on 1 April 2022 also adopted an expanded approach in permitting service of orders out of jurisdiction. The Singapore Court would consider if there is a good arguable case that there is a sufficient nexus to Singapore (Paragraph 63(2)(a), Supreme Court Practice Directions 2021, "SCPD"), and would consider

"*if the application is for the production of documents or information (i) to identify potential parties to proceedings before the commencement of those proceedings in Singapore; (ii) to enable tracing of property before the commencement of proceedings in Singapore relating to the property*" (Paragraph 63(3)(u), SCPD). While there have not been any reported judgments, the English position is likely to be adopted under this expanded gateway to permit the service of *Bankers Trust* orders and *Norwich Pharmacal* orders out of jurisdiction.

FREEZING ORDERS IN THE FORM OF NFTS: ENFORCING ORDERS AGAINST CRYPTOASSETS A CLAIMANT DOES NOT HAVE ACCESS TO

Obtaining a freezing order / injunction in respect of the cryptoassets and judgment against a fraudster is an important milestone for any claimant in a crypto-related dispute. However, it is only half the battle won in terms of asset recovery. How can the order / injunction / judgment be enforced if the claimant does not have access to the cryptoassets in question?

The transfer of and access to cryptoassets are controlled by a set of digital keys and addresses. While anyone is able to transfer cryptoassets to any public address, the recipient must have a unique private key to access the received cryptoassets. Private keys can be kept in custodial wallets (e.g., with a crypto exchange) or in non-custodial wallets (where one stores one's own private keys). Both types of wallets can be hot (connected to the internet) or cold (not connected to the internet).

As transfers of cryptoassets are recorded on the public blockchain ledger, it is possible to trace the last known location of the cryptoassets and whether they reside at an address associated with a custodial wallet (with a crypto exchange) or a non-custodial wallet (e.g., a cold wallet).

Where the defendant or the third party (or crypto exchange) in possession of the wallet is known, and a court order has been made over the cryptoassets which require keys to access, the private keys can be obtained through discovery procedures, *i.e.*, the claimant can seek disclosure of the private keys from the defendant or the third party (or crypto exchange) during

enforcement. This would be largely analogous to traditional enforcement of orders against moneys held by a bank or financial institution. Claimants need to be aware that the third party / crypto exchange might not cooperate, and that they may have to adopt other strategies to pressure the platforms to voluntarily comply with such court orders.

Where cryptoassets are controlled by overseas exchanges, it is also possible for the court to order that they be transferred into the court's control in order to facilitate with future enforcement. This would allow the claimant to avoid issues concerning access to the private keys discussed above. In *Joseph Keen Shing Law v Persons Unknown & Huobi Global Limited* [2023] 1 WLUK 577 ("*Joseph Keen*"), the claimant had obtained a worldwide freezing order and a default judgment against the fraudsters. The London Circuit Commercial Court considered that while Huobi had not permitted the fraudsters to access the accounts (and Huobi had indicated an intention to cooperate with any order made by the English Court) that "*may not necessarily occur and continue to be the case, and of course the court has no control over any of the relevant defendants, all of whom are based exclusively outside the jurisdiction of this court.*" (*Joseph Keen* at [11]) The Court therefore found it appropriate to order the transfer the funds subject of the worldwide freezing order into jurisdiction, and for Huobi to convert the cryptoassets to fiat currency and credit them to the claimant's solicitors, or to credit the cryptoassets to the claimant's solicitors who will convert them into fiat currency (to be onwards transferred into the client account or to the court's office: *Joseph Keen* at [24]).

It is more challenging, however, where the cryptoasset is associated with keys kept in a cold wallet in the possession of an unknown party. However, not all is lost. Fraudsters may seek to extract value from cryptoassets by transferring them to other parties or by converting them to fiat currency, and such transactions would involve hot wallets, and become recorded on the public blockchain ledger and traceable. Claimants can then seek information and take action against the hot wallets and exchanges involved. It would nevertheless require more time and effort to monitor the movement of such cryptoassets.

In this regard, the Singapore High Court recently granted a worldwide freezing order in the form of an NFT (unreported). The order was tokenized

and permanently attached to the cold wallets in question. While the NFT in itself does not stop transactions, the intention was for the NFT to serve as a warning to third parties that the wallets in question are subject of a hacking incident and the order. The party who obtained the order also designed a process to track funds leaving the wallets.

CLAIMS AGAINST CRYPTO EXCHANGES ON THE BASIS THAT THEY HOLD STOLEN CRYPTOASSETS IN TRUST

Constructive Trust

The Singapore High Court in *ByBit Fintech Ltd v Ho Kai Xin and ors* [2023] SGHC 199 recently held that cryptoassets are property in the eyes of the law, such that a wrongdoer can be found to be holding the cryptoassets on constructive trust for a claimant.

In that case, an employee of an external payroll company engaged by ByBit Fintech Ltd ("ByBit"), a crypto exchange, had wrongfully transferred, among other things, 4,209.720 USDT to four crypto addresses controlled by the employee. The Singapore High Court found that the wrongdoer employee held the USDT on institutional constructive trust for ByBit, and that institutional constructive trust arose by operation of the law as a result of unconscionability (such as fraud and profiting from a breach of fiduciary duty).

In the UK, claimants have attempted to apply similar arguments, not against the wrongdoer, but against crypto exchanges.

In *Piroozzadeh v Persons Unknown and ors* [2023] EWHC 1024 (Ch) ("*Piroozzadeh*"), a claimant traced stolen USDT to wallets in accounts registered with Binance. The claimant then obtained a without notice interim injunction against Binance on the basis that it held the stolen USDT on constructive trust for the claimant. Binance succeeded in having the without notice order set aside on the basis that the claimant failed to comply with its duty of full and frank disclosure:

a. The claimant omitted to inform the court that Binance could raise the defence that it was a bona fide purchaser of the transferred asset (as it was not involved in the fraud); and

b. The claimant failed to inform the court that Binance's practice was to transfer all cryptoassets it received into a pool. In other words, Binance mixed its customer's assets. The lack of segregation made tracing "essentially futile and close to impossible and possibly impossible exercise" (Piroozzadeh at [8]). The claimant was aware of this as Binance had raised this in its defence in separate but similar proceedings that the claimant had copies of (Piroozzadeh at [29], [38]-[39]).

While Binance succeeded in setting aside the without notice interim injunction, this does not mean that a claim in constructive trust against a crypto exchange is bound to fail.

Whether such a claim would succeed depends on the extent to which the crypto exchange was put on notice of the wrongdoing and how the cryptoassets are held by the crypto exchange. There have been more instances of crypto exchanges collapsing as a result of their own fraud. In such cases, it may be possible for claimants to contend that the wrongdoing on the part of the crypto exchange gives rise to a constructive trust in the claimant's favour.

Express trust

Conversely, if the crypto exchange was not put on notice of any wrongdoing, it might be able to raise the defence that it was a *bona fide* purchaser of the deposited asset (as in *Piroozzadeh*). Under common law, a *bona fide* purchaser for value of a property without notice of existing prior claims to the title would take good title to the property, even if the property was fraudulently obtained by the seller.

In a case of an insolvency where no fraud is involved, one may consider whether an express trust has been created in the claimant's favour when seeking to recover cryptoassets that have been deposited at addresses linked with wallets held by crypto exchanges. Under Singapore law, three certainties are required for the creation of an express trust:

> *"**Certainty of intention** requires proof that a trust was intended by the settlor. While no particular form of expression is necessary, there must be clear evidence of an intention to create a trust. Next, the trust must **define with sufficient certainty the assets** which are to be held on trust and the interest that the beneficiary is to take in*

them. Finally, ***certainty of objects*** *requires clarity as to the intended beneficiaries so it is possible to ascertain those who have standing to enforce the trustee's duties under the trust*." (*Cheng Ao v Yong Njo Siong* [2023] SGHC 22 at [35])

In cases involving cryptoassets involving crypto exchanges, certainty of intention is reflected from:

a. The terms governing the relationship between the customer and the exchange: Where the terms provided that customer deposits were held on trust by the exchange, an express trust can be found to exist (Ruscoe v Cryptopia Ltd (In Liquidation) [2020] NZHC 728, "Ruscoe"). On the other hand, if the terms contain clauses that provide for rights of ownership (such as the ability to pledge, hypothecate or lend) that can be exercised by the exchange, indicate the absence of a trust (In re Celsius Network LLC, 647 BR 631 (Bkrtcy SDNY 2023)); so would terms stating that the exchange did not take client fund safety measures (such as depositing client assets in a trust account) and that it would not be able to return customer assets in the event of bankruptcy (Quoine Pte Ltd v B2C2 Ltd [2020] 2 SLR 2020).

b. The behaviour of the exchange: The lack of segregation and the exchange's use of customer assets as though they belonged to the exchange would reflect a lack of intention to create a trust. How the exchange treats the assets in its financial accounts would also be considered. In Re Gatecoin Limited (in liquidation) [2023] HKCFI 941, the exchange included customer assets in its financial statements (which reflected a lack of intention to create a trust), whereas in Ruscoe, the exchange did not incorporate customer assets when filing its financial accounts and tax returns, and a trust was found to exist.

Turning back to Singapore, this issue may be less murky by next year. The Monetary Authority of Singapore has recently required all Singapore crypto service providers to deposit customer assets under a statutory trust before 2024. The aim is to mitigate the risk of loss or misuse of customers' assets and facilitate the recovery of customers' assets in the event of an insolvency.

BLOCKCHAIN DEVELOPERS MAY OWE FIDUCIARY / TORT-BASED DUTIES TO CLAIMANTS

In *Tulip Trading Limited (A Seychelles Company) v Bitcoin Association For BSV & Ors* [2023] EWCA Civ 83 ("*Tulip*"), the English Court of Appeal thought it arguable that cryptoasset software developers owed fiduciary and tort-based duties to owners of cryptoassets utilising their network. This was a preliminary determination and the matter would be decided at trial.

In that case, the private keys to US $4 billion worth of Bitcoin were lost in an apparent hack. The claimant contended that the 16 named software developers controlled and ran four Bitcoin networks and were able to secure the stolen Bitcoin by moving them to another address that the claimant could control. Unsurprisingly, the software developers contended that the Bitcoin networks were decentralized and "*part of a very large, and shifting, group of contributors without an organisation or structure*". Further, any change proposed would be ineffective as the miners would refuse to run it, and a disagreement would result in a "*fork*" (*ie*, the creation of additional networks) (*Tulip* at [33]). The English Court of Appeal eventually stated that this would be an issue to be resolved at trial (*Tulip* at [91]).

Each type of cryptoasset is created and issued within its own network. There are decentralized networks without any central network owner (like Bitcoin) and centralized networks where there is a central network owner.

In *Tulip*, the software developers were able to contest the claimant's argument that such duties existed by relying on the fact that the Bitcoin networks are *decentralized* and that they would not be able to implement the change requested by the claimant. However, where the cryptoasset network in question is *centralized* (*i.e.* where there is only one software developer controlling the entire network), it may well be that it is more likely that such duties would arise. As the English Court of Appeal noted in *Tulip*, "*developers are people who it is clearly arguable have undertaken a role which at least bears some relationship to the interests of other people*" and, in a cryptocurrency situation, have authority given to them by their control of access to the source code, and are "*in effect making decisions on behalf of all the participants in the relevant*" network. These features are common to fiduciary duties currently recognized by the law, and make it possible for developers of centralized networks to be found to owe fiduciary duties to claimants (*Tulip* at [70]-[76]).

AUTHORS

Wendy Lin

Fellow Wendy Lin is the Deputy Head of the Commercial & Corporate Disputes Practice, and a Partner in the International Arbitration Practice at WongPartnership LLP.

Leow Jiamin

Leow Jiamin is a Partner in the Commercial & Corporate Disputes Practice at WongPartnership LLP.

Share This Read

Due Diligence

Enhancing Pre-Transaction Due Diligence in CEE/SEE : Three Areas Where a Conventional Balance Sheet Review Falls Short

JITKA LOGESOVÁ

JAROMIR PUMR

Introduction

Anticorruption and compliance due diligence is still being conducted only in a limited number of cases as a part of pre or post-acquisition due diligence in Central Eastern Europe and South Eastern Europe (CEE/SEE). Limited or inaccurate due diligence prior to an acquisition can significantly weaken the (negotiation) position of clients and sometimes very seriously impact the business of the acquired company. Due diligence that fails to account for compliance risks or does not approach risks holistically often leads to considerable post-acquisition losses, sometimes even necessitating a complete write-off of the target company. The following article aims to point out some of the current key considerations and risks stemming from the expanding regulatory frameworks throughout in CEE/SEE.

REDEFINING RISKS: DYNAMIC EVOLUTION IN REGULATORY FRAMEWORKS AND ENFORCEMENT

When assessing transaction risks, usually three main categories of risks are being targeted: business, regulatory and reputational. For a long time, these risks were generally considered independently of one another during due diligence processes. However, as the world becomes more interconnected on the one hand, yet more regulated and less globalized on the other, we are seeing various specific risks increasingly intersect and overlap. Furthermore, the category of regulatory risk is now more likely to encompass risks that were purely seen as business or reputational risks in the past, or even entirely new risks. These include for example corporate criminal liability, sanctions, money laundering, undisclosed ultimate beneficial owners (“UBO”), conflicts of interest, bribery, bid-rigging, money laundering, tax, GDPR compliance and HR related risks like harassment or mobbing. Recent years have brought an avalanche in regulatory oversight, not only on the national level but also – and more importantly – on the multi-national level, with coordination among key jurisdictions such as the USA and the EU.

This situation has resulted in a challenging scenario for both traditional, long-established businesses and startups. The former are scrambling to

implement a whole array of new regulations into their large-scale processes across different jurisdictions, many of which they may never get round to implementing. Meanwhile, early-stage companies tend to pay less attention to regulatory compliance. Both types of business might then bury certain risks within the fabric of their company, often hidden deep below the surface.

It has been relatively common for acquisition due diligence not to catch red flags, even when the target's business practice clearly qualified as a complex bribery scheme under the law of the target's home country. The number of such cases has been on the rise for some time, particularly because the definition of bribery in many European countries is quite broad and covers both public and private bribery (passive and active). In the region, it is quite common for employees or board members to have a reporting obligation if they come across a suspicion of bribery post-acquisition. Consequently, the employees or board members cannot just sweep it under the rug; they have a personal, legal duty in many circumstances to report immediately to the authorities.

The key issue with regulatory risk, including bribery, is that it can significantly worsen the investor's position or even lead to a write-off of the investment. Unlike reputational or business risk, regulatory risk tends to attach itself to the company and its assets and in some cases can make the acquiring company "toxic". In another recent case, we saw how corporate criminal liability transferred to the acquiring company through an acquisition of "significant assets."

This convergence of business and reputational risk with regulatory risk illustrates the need to change mindsets when conducting pre-transactional due diligence. Red-flag issues that go unnoticed or are mismanaged before a transaction can expose investors to criminal or civil litigation both on a corporate and individual level.

CORPORATE CRIMINAL LIABILITY AFFECTS TARGET COMPANY AND ITS ASSETS

In Czech Republic and many other CEE/SEE countries, a company is responsible for almost all crimes listed in Criminal Codes, which can be committed by a wide spectrum of personnel, including managers, employees,

board members, and shadow directors. Criminal liability is incurred not only if the crime is carried out in the company's interest but also as part of its commercial activities. This means that the company can also become the offender if they are damaged by the act. For example, we had a client recently that was defrauded in a double invoicing scheme, which led the client's company to be charged with tax fraud for deducting non-incurred costs. The company's liability can be based solely on the actions and intent of the individual perpetrator, and it remains separate and concurrent with the individual's criminal liability. The individual need not even be identified. A concern is that sometimes employees or the company unknowingly engage in illegal activities, either because this is what they learned to be "business-as-usual" or even because the company was a victim of a fraud.

Moreover, the Czech case law concluded that criminal liability may extend not only to the legal entity but also to its key assets. This in practice means that if the criminally liable company sells its key assets to another company, both can face criminal charges and sanctions. Therefore, criminal liability can effectively make the assets of a company "toxic", where liabilities attached to acquired assets can emerge up to several years after their acquisition and can not only block the acquiring company from disposing of the acquired company or its assets but may also result in sanctions being imposed on the company who acquired the tainted assets. The sanctions in Czech Republic often include ban on commercial activities or a prohibition on fulfilling or participating in public tenders. This means that the mitigating efforts of restructuring the target company or selling its assets may not prove fruitful, and that the company acquiring tainted assets may also face devastating sanctions of ban on part of its commercial. This risk underscores the importance of conducting a comprehensive review of the target company's history and operations to uncover any criminal activities or liabilities.

TYPICAL DUE DILIGENCE IN THE CEE/SEE REGION

In the M&A environment in CEE/SEE, there is a noticeable inclination towards pursuing cost-effective and predominantly financial due diligence processes ("a desktop review," consisting of remote review of documents that have been agreed, selected and prepared beforehand). This approach is of course often driven by budgetary constraints and a traditional perspective of due diligence

in which the primary goal is to evaluate the financial health and viability of the target company. This due diligence typically involves reviewing financial statements, assessing assets and liabilities, analyzing historical financial performance, and conducting legal review of key contracts and obligations.

These documents, such as audit and financial reports, primarily offer a historical view of a company's financial performance. They are excellent for understanding past profitability, revenue trends and financial stability. However, they do not capture non-financial factors. Contracts and current litigations cannot typically be relied upon to assess the robustness of the legal and compliance processes currently in place at a target company. Issues such as a company's culture and any conflicts of interest involving its key personnel are usually overlooked.

There is also an overreliance on self-reported information and professional memorandums, opinions, or advice. Gathering relevant information is undoubtedly a difficult task, especially in a less-than-friendly takeover. However, this self-reported information might not always present a complete or entirely accurate picture, especially in areas where subjective judgment or undisclosed information (like internal conflicts or ethical practices) play a role. Additionally, much of the information gleaned from audits and reports is based on data provided by the target company itself or produced for its benefit by its trusted advisors. While these can provide valuable insight and advice, they are not always correct and are never binding for law enforcement or tax authorities. Occasionally, we have seen how incorrect advice can lead to significant damage to materialize many years in the future.

The most frequent lesson learned from our practice is that a traditional "desktop review" is unable to identify certain compliance risks because the company looks great on paper. These areas included corporate criminal liability, tax and specific regulatory risks (money laundering, sanctions, various reporting areas such as DAC6 or ESG). In the CEE/SEE region, a significant challenge within the M&A sector is the limited awareness and understanding of the importance of compliance due diligence. Based on a tailored risk assessment, compliance due diligence involves a thorough assessment of how well the target company and its key personnel adhere to relevant laws, regulations and industry standards.

Compliance due diligence is feared because it is inherently a very broad topic. However, it is not necessarily an expensive and demanding exercise and, in many cases, can be done by the buyer itself. The issue, predominantly, is that it is not part of regular practice and is not well known. Simple compliance due diligence of a target company consists of two parts. The first is the initial risk assessment, which is crucial for understanding the target company's specific risk profile: the company's business environment; industrial sector; the extent of its international operations, products and services offered; business processes; IT infrastructure; and sales channel. The second part consists of a review of high (and medium) risk areas, alongside the due diligence. Depending on the risks, this involves background checks of selected business partners and suppliers, transactions, key personnel or stakeholders, as well as their interviews.

How to handle compliance diligence reporting

In most cases, compliance due diligence does not identify serious risks or issues. It points out any deficiencies or red flags, which in turn increases the negotiation leverage of the buyer. When critical issues are detected, the easiest approach might be to walk away from the transaction altogether. However, there will be other cases where this is not possible, or the transaction is too important to the buyer. In these cases, additional indemnities or warranties are highly recommended. In other cases, companies often consider self-disclosure.

In CEE/SEE region, companies also need to be aware of the duty to report, which is a legal obligation to immediately report (or prevent altogether) a catalogue of crimes to the enforcement authorities. Non-reporting is a crime. Most often, the duty to report a crime falls on the individuals, for example company's employees or advisors. Therefore, if there is a risk that reporting duty can be triggered during the compliance due diligence either pre or post-acquisition, the person should immediately stop reviewing the data or a report and an independent attorney should be engaged to review the issue (attorneys are generally exempt from the reporting duty).

As for remediating the misconduct, in the USA, for example, the Department of Justice announced a Mergers & Acquisitions Safe Harbor policy on 4 October 2023, to promote voluntary disclosure of criminal misconduct in acquired companies. Eligible companies must report any misconduct within six months of closing an M&A deal and remediate the misconduct completely

within one year. In the CEE/SEE region, on the other hand, existing legal frameworks often present a challenge as they hinder cooperation between prosecuting authorities and companies that are willing to collaborate or self-disclose. Usually, the law provides no automatic benefit for self-disclosure or cooperation, nor does it incentivize companies to self-report and cooperate with prosecuting authorities.

In this sense, companies cannot be certain that they will obtain any benefit should they decide to cooperate, share information, or report misconduct. For example, in Czech Republic, the only viable option for companies is a Guilt and Sanctions Agreement made between the offender and the public prosecutor. The offender must admit that the facts as presented by the prosecution are correct and agree to sanctions. However, the defendant has no legal instrument to influence the bargaining process, thus the public prosecutor has the upper hand. In practice, public prosecutors do not offer many benefits and are unwilling to offer many concessions. The biggest upside of this instrument is that if the company can negotiate to be sentenced with a monetary fine only, it can avoid having a criminal record because by paying the fine, the company is regarded as if it had not been convicted.

CONCLUSION

The significant shift towards new and extended regulations in previously unregulated areas requires a change in due diligence mindsets. Compliance due diligence is critical for detecting situations that look great on the paper but pose significant risks to the buyer that a desktop review cannot detect. In the CEE/SEE region, those mostly include the transfer of criminal, tax, or regulatory liability through “tainted assets” to the buyer(s). Despite the importance of compliance due diligence, there remains a lack of awareness regarding its value and utility. Nevertheless, a brief background search can be instrumental in uncovering issues that might otherwise lead to big losses or cause an investment/exit strategy to fail because of the non-transferable tainted assets. The implementation of whistleblowing directives in the EU has resulted in a rise in whistleblower activity. Unfortunately, however, whistleblowers may be of little help to a buyer, as very often whistleblowers report issues only after a transaction has been concluded.

AUTHORS

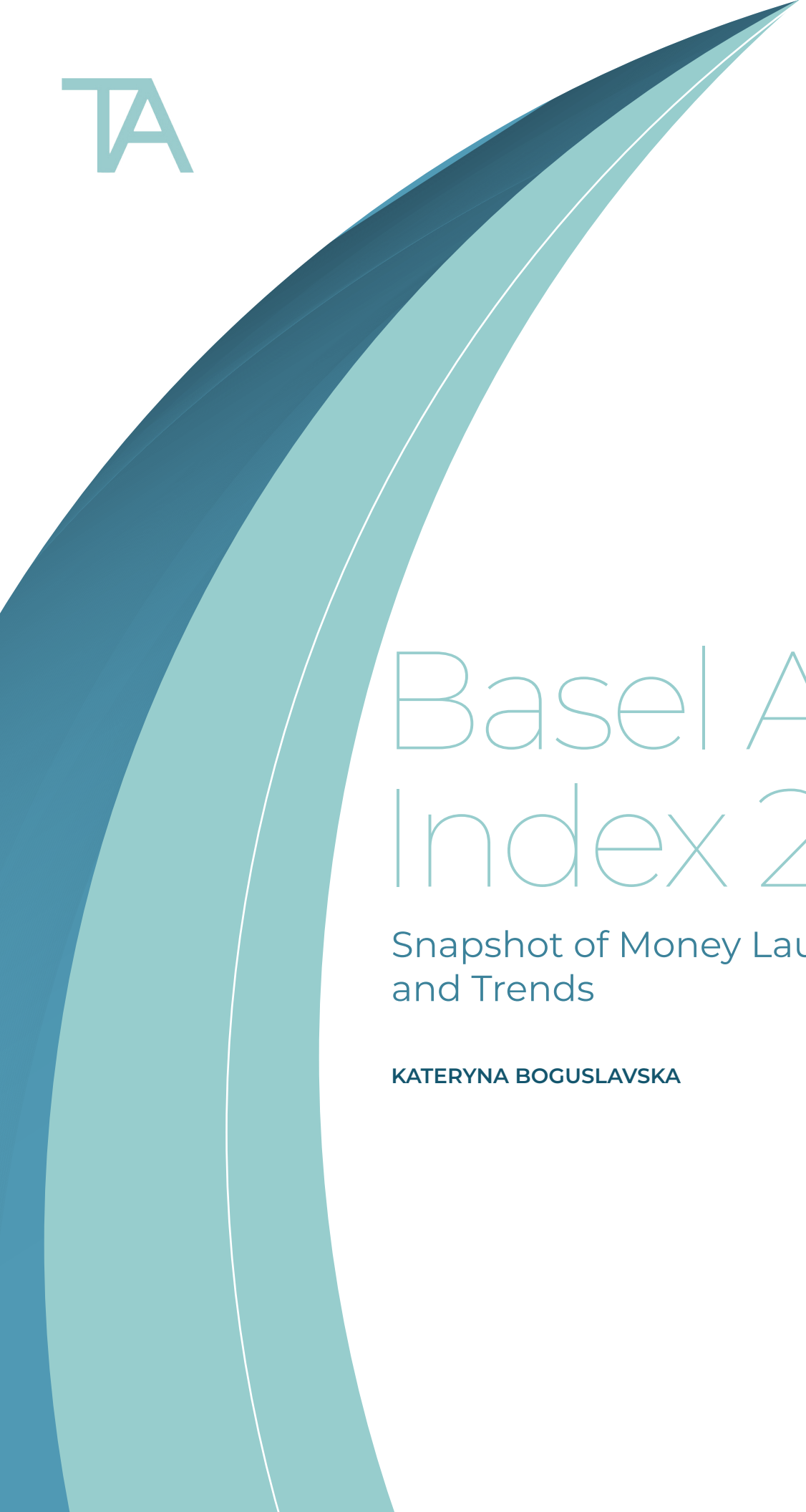
Jitka Logesová

Fellow Jitka Logesová is Managing Partner in Wolf Theiss Prague and leads the firm-wide Investigations, Crisis Response and Compliance Practice. She specialises in compliance, corporate investigations, corporate criminal liability/white collar crime, sanctions and asset recovery.

Jaromir Pumr

Jaromír Pumr is an Associate in Wolf Theiss. He specializes in corporate governance, compliance and crisis response. He is an expert in the areas of corporate investigations, white-collar crime, anti-corruption, money laundering and sanctions.

Share This Read



Basel AML Index 2023:

Snapshot of Money Laundering Risks and Trends

KATERYNA BOGUSLAVSKA

Introduction

Why are governments so challenged to implement financial sanctions? How are terrorist groups able to receive the financing to launch horrific attacks – why weren't these transfers detected and halted? What on earth is happening with cryptocurrencies? And why are less than one percent of illicit financial flows estimated to be intercepted and recovered?

These questions are among those explored in the 2023 Basel AML Index Public Edition report, released on November 13, 2023 for the 12th year running. This year, due to increased data availability, 152 countries were covered in the Public Edition.

The Basel AML Index is widely known and respected as an independent ranking of money laundering and terrorist financing (ML/TF) risks around the world. It is a composite index that provides risk scores for countries based on data from 18 publicly available sources in five categories:

1. Quality of anti-money laundering and counter financing of terrorism (AML/CFT) framework
2. Bribery and corruption
3. Financial transparency and standards
4. Public transparency and accountability
5. Legal and political risks

Journalists tend to go straight to the public ranking to see who's at the top and bottom of the risk scale, whether their country has improved or worsened since the year before, and how it stands in relation to its neighbors.

But we have long encouraged users to go beyond that "good country, bad country" approach – not least because small changes from year to year are often statistically insignificant or a result of a small methodological tweak – and to explore the data behind the ranking.

Below is a short overview of this year's key findings and what data on ML/TF can tell us about global events. Find more on the website and in the report (in the Downloads section).

THE BASEL AML INDEX – AN OVERVIEW

The aim of the Basel AML Index is to provide a holistic picture of ML/TF risk. Risk, as measured by the Basel AML Index, is defined as a jurisdiction's vulnerability to ML/TF and its capacities to counter it. It is not intended as a measure of the actual amount of ML/TF activity in a given jurisdiction.

The 18 indicators differ in focus and scope in order to create this holistic picture. Data from individual indicators is collected and normalized on a 0–10 scale, where 10 indicates the highest risk level. Each of the indicators is given a weight in the overall score depending on its relevance to assessing ML/TF risk. For example, Financial Action Task Force (FATF) evaluations make up 35 percent of the overall score as a major source of information on the quality of a country's AML/CFT framework. Conversely, indicators of the rule of law and judicial independence each correspond to only 2.5 percent of the overall score; while important, they are less directly relevant to assessing ML/TF risk.

The indicators and weighting are reviewed annually by an independent expert group. The full methodology and list of indicators are available on the Basel AML Index website (methodology page).

GENERAL TRENDS

Standout findings this year were rather depressing. First, the average global risk of ML/TF across all 152 countries increased slightly from 5.25 in 2022 to 5.31 this year. This is on a scale from 0–10, where 10 is the maximum risk. Though the change is small, it indicates that efforts to crack down on ML/TF are still not having enough impact.

Why aren't they having enough impact? One reason may be an apparent fall in *effectiveness*. Our analysis of data from the FATF shows a continued decline in the measured effectiveness of AML/CFT systems globally. Scores dropped from the already low level of 30 percent effectiveness to 28 percent.

Some of the biggest problem areas in terms of effectiveness are those that are most critical to the world right now: the misuse of non-profit organizations for terrorist financing, transparency of beneficial ownership information, and the quality of supervision of both financial institutions and

designated non-financial businesses and professions (including lawyers). Efforts to prosecute those who commit ML/TF offenses and confiscate illicit assets are also languishing.

Beyond FATF data and indicators of the "quality of AML/CFT framework" specifically, we also saw increased risk scores in all four other domains measured by the Basel AML Index: corruption and bribery, financial transparency and standards, public transparency and accountability, and legal and political risks.

THREE FOCUS AREAS

Though sometimes questioned over issues of transparency, the FATF evaluations provide the most robust and quantitative data on specific aspects of AML/CFT policy and implementation. This year, we looked at what the data says about three areas of particular pertinence given global events:

Confiscation: the missing key to preventing crime

Our analysis shows that countries' law enforcement authorities are doing fairly well at identifying and freezing illicit funds and other assets during investigations. (In the West, the recent rush to identify and freeze assets of sanctioned individuals and the Russian state in connection with the Russian invasion of Ukraine likely gave this a boost.) Technical compliance with the FATF's Recommendation 4 on confiscation is high at 76 percent, with no jurisdictions assessed as non-compliant.

But the data also shows that we are not managing to permanently confiscate enough illicit assets to create a deterrent effect. Globally, measures to confiscate illicit assets are just 28 percent effective, according to the FATF's Immediate Outcome 8. The score has remained static since last year. Just five of the 161 assessed jurisdictions demonstrate a high level of effectiveness in confiscation.

What's more – as we know from our own experience at the Basel Institute supporting law enforcement agencies in their asset recovery efforts – confiscations are even rarer when assets are hidden in a foreign jurisdiction. This may be because of mediocre scores for mutual legal assistance with regard to

the freezing and confiscation of assets. According to FATF Recommendation 38 on mutual legal assistance, the global average for compliance is 66 percent, with less than 20 percent of countries fully compliant.

Our conclusion: stronger laws will help, but they won't solve problems with the implementation of those laws and with cross-border cooperation through mutual legal assistance.

However, a recent decision at the FATF's October 2023 plenary session may give confiscation outcomes a boost. Delegates agreed on major amendments to the FATF Recommendations that will, among other things, require states to:

- have policies and operational frameworks that prioritize asset recovery;
- establish non-conviction based confiscation regimes to facilitate the recovery of assets without a criminal conviction;
- have the power to suspend transactions related to money laundering, terrorist financing and serious crime.

These will take time to show up in the data. But we look forward to anything that will facilitate the detection and confiscation of illicit assets and their return to victims and victim states.

New technologies: what to do with virtual assets?

The crypto industry continues to hit the headlines with its breathtaking volatility and billion-dollar scandals. The news (though this was known for years) that terrorist groups such as Hamas had received funding via cryptocurrencies also gave policymakers a jolt.

Here, our analysis shows that compliance with the FATF's Recommendation 15 on new technologies – covering virtual assets and virtual asset service providers (VASPs) – has plummeted since the FATF strengthened its requirements. Average compliance levels have dropped from 63 percent in 2021 to 43 percent today. This is the second weakest of all 40 Recommendations after non-profit organizations (see below).

In the report, we point out that it is natural for regulators to be unsure how to react to the fast-evolving industry and its inherent risks and opportunities.

(Academy Fellow Dorothy Siron co-authored a most interesting Working Paper on this topic with our crypto lead Federico Paesano last year: *Cryptocurrencies in Asia and beyond: law, regulation and enforcement*.)

We also point to encouraging signs, such as stronger and more joined-up regulations in the E.U. and the amount of illicit virtual assets that law enforcement authorities in the U.S. and beyond are recovering.

But our message is strong: countries everywhere cannot relax. They need to move fast and firmly to understand the evolving financial crime risks of new technologies like cryptocurrencies and regulate/enforce appropriately in line with a risk-based approach.

Misuse of non-profit organizations for terrorist financing

The last of our three "deep dive" analyses looked at data on the misuse of non-profit organizations to fund terrorism. This is a topical issue right now, but also a long-running debate due to the unintended consequences of heavy-handed implementation of the FATF's Recommendation 8 on non-profit organizations.

This year, average compliance with Recommendation 8 is just 41 percent – the lowest level of all Recommendations. Effectiveness scores according to the FATF's Immediate Outcome 10 are also below average at 25 percent. Regions struggling with terrorism, including Sub-Saharan Africa and Southeast Asia, have worryingly low scores for effectiveness at just 2 and 8 percent respectively.

The report points out several things that public authorities, financial institutions, and non-profits themselves can do to build resilience against the abuse of this sector for terrorist financing. However, our analysis warns that simply increasing controls on *all* non-profits is not the way forward. It puts at risk the legitimate work of non-profits dedicated to helping the world's most vulnerable people – potentially endangering vital humanitarian assistance and violating human rights.

Again, the key lies in a risk-based approach: properly understanding *which* organizations are vulnerable, in *what way* they are vulnerable, *how* terrorists abuse these organizations, and applying resources accordingly.

CONCLUSION: RISKS AND REAL PEOPLE

Throughout this year's Basel AML Index Public Edition report is a constant theme: the need for a risk-based approach to ML/TF based on a thorough assessment of each country's or sector's specific context and threats.

We also wish to stress that AML/CFT is not just a technical field. All three focus topics illustrate how AML/CFT deficiencies impact economic prosperity, security, and sustainable development. Building resilience to ML/TF is not only about getting good scores from the FATF and Basel AML Index, but about preventing harm to people and the planet. It is also key to building a well-functioning society and economy based on trust, transparency, and the rule of law.

AUTHOR

Kateryna Boguslavska

Kateryna Boguslavska is the Basel AML Index Project Manager, Basel Institute on Governance.

Share This Read

UK Sanctions:

A Review of 2023 Key Challenges and Trends

MARIA NIZZERO

Introduction

Since Russia's full-scale invasion of Ukraine on February 24, 2022, the United Kingdom has joined the United States and other allies in an unprecedented, coordinated sanctions response. Then UK Foreign Secretary Liz Truss emphasized the country's unwavering commitment to intensifying pressure on individuals linked to the Kremlin and other key enablers, targeting not only their businesses, but also their assets and lifestyle, as long as Russian forces maintained a presence in Ukraine.

As of August 2023, more than 1,600 individuals and 230 entities have been subject to UK sanctions under the *Russia (Sanctions) (EU Exit) Regulations 2019* (Russia Regulations). Among them, at least 129 "oligarchs", with a combined net worth of over £145 billion, have been subject to this targeted approach, the House of Commons Library reports. In the meantime, this unprecedented response has also led to challenges in English courts. Since 2021, more than 30 individuals have requested a revision of their designation, whether under the Russia Regulations or other regimes.

As cases start to be appear in court, they highlight a very low threshold when it comes to the designating process, but a high bar when it comes to challenging said designation. At the same time, while the designation process itself is hardly questioned by the courts, the enforcement of the sanctions regime is put to test. This article explores challenges and trends that have characterized the UK sanctions landscape in 2023. In particular, it focuses on key landmark decisions involving sanctioned individuals, as well as policy developments in the UK aimed at improving sanctions implementation.

A BROAD REMIT FOR DESIGNATING - A HIGH BAR FOR CHALLENGING.

The year 2023 has witnessed a series of landmark decisions regarding sanctions designations, both in the context of the Russia Regulations and relating to the broader UK sanctions landscape. Three cases in particular underscore a prevailing trend surrounding the considerable leeway granted

to the Foreign, Commonwealth and Development Office (FCDO) in making designations: *LLC Synesis v Secretary of State for Foreign, Commonwealth and Development Affairs* [2023] EWHC 541(Admin) (*Synesis*), *Eugene Shvidler v Secretary of State for Foreign, Commonwealth and Development Affairs* [2023] EWHC 2121 (Admin) *(Shvidler)*, and *Mints v National Bank Trust and Bank Okritie* [2023] EWCA Civ 1132 (*Mints*). These cases also clarify key issues in sanctions designation processes, including the concept of "involved person", the standard of proof and the type of evidence that can be used by the decision-maker for the designation, and the concepts of "ownership" and "control".

The *Synesis* case, albeit not concerning the Russia Regulations, laid the foundations for ensuing challenges. In this case, the court rejected a designation challenge under section 38 of the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). The court upheld the FCDO's decision not to remove Synesis from the list of designated persons, emphasizing its role in scrutinizing procedural aspects of the designating process rather than "standing in the shoes" of the decision-maker in relation to the evidence on which the designation is made. The court also confirmed that:

a. historic behavior could still be subject to sanction, and as such an individual or entity can still be considered an "involved person", and therefore designated, even if they are no longer actively engaged in the sanctionable activity;

b. the statutory threshold applied by the FCDO for designations extends beyond mere "reasonable grounds to suspect", to include (i) hearsay, (ii) multiple hearsays, (iii) allegations, and (iv) intelligence. Crucially, the decision-maker is only required to evaluate the available information in good faith; and

c. the role of the court when making its review under Article 38 of SAMLA is only to examine whether the decision-maker's decision was either based on no evidence or was irrational, and not to make a judgment itself.

The *Synesis* case serves as a significant indicator of the low bar given to the executive in matters of designation processes, and the little that courts can do about it.

The same trend was reflected in the *Shvidler* case, the first legal challenge to a designation under the Russia Regulations brought by Eugene Shvidler. Shvidler was designated right in the aftermath of Russia's invasion of Ukraine on the grounds he was an "involved person", due to his alleged ties with Roman Abramovich and past association with Evraz PLC, a company accused of aiding the Russian war effort.

The court's ruling mirrors in many ways the *Synesis* case:

a. The court confirmed the lower threshold for imposing sanctions, as long as the decision is reasonable and proportionate. It also rejected Shvidler's argument that personal suffering caused by sanctions should outweigh designation even in cases when "the foreign policy objectives (...) are of the highest order".

b. The court held that the imposition of sanctions serves as a message to the designated individual and others in a similar position surrounding their conduct.

c. The court confirmed that historic behavior can still be subject to sanction. In particular, in response to Shvidler's argument that he had condemned Russia's actions in Ukraine, Mr. Justice Garnham held that "the value of [the] messages [of a sanction designation] persists even if the person in question ceases the conduct complained of and makes statements distancing himself from the Russian regime".

The English courts have also implied that broad scope should not limited to the kind of evidence the FCDO can assess when imposing sanctions or to the concept of "involved person", but also to the concept of "ownership" and "control". On October 6th, 2023, the Court of Appeal handed down judgment in the case of *Mints*, in which it included comments on the control potentially exercised by President Putin, who was personally sanctioned by the UK government after the invasion of Ukraine, over the Russian economy. In this context, the influence wielded by President Putin by virtue of his political office was considered so significant that "the consequence might well be that every company in Russia was 'controlled' by Mr. Putin and hence subject to sanctions". OFSI and the FCDO published a statement shortly after the judgment, noting that "[t]here is no presumption on the part of the Government that a private entity based in or incorporated in Russia or any jurisdiction in which a public official is designated is in itself sufficient evidence to demonstrate that the relevant official exercises control over that entity".

HIGHLY LITIGIOUS AND HIGHLY EVASIVE

The imposition of sanctions and recent court judgments have not deterred designated entities and individuals from utilizing English courts to pursue litigation. This point has also been made in the Mints case, which confirmed that designated persons could not be excluded from the English courts. More than 30 sanctioned individuals have sought a government review of their designations since 2021, while others have challenged the National Crime Agency's (NCA) investigations into alleged sanctions evasion. This raises questions, if not on the robustness of UK sanctions designation processes, then on the effectiveness of its sanctions enforcement.

Beside the case of Shvidler, whose lawyers announced he would appeal, Petr Aven, the former director of Russian banking giant Alfa Group, contested a NCA investigation on suspected sanction evasion. In *NCA v. Westminster Magistrates' Court* [2022] EWHC 2631 (Admin), Aven demanded the reversal of two Account Freezing Orders (AFOs), citing the NCA's "chaotic and unprincipled approach" and asserting that there was no reasonable basis for any "purported suspicion" of the offense being committed. In July 2023, the Westminster Magistrates' Court ruled that the frozen funds could be used to cover some of Aven's expenses, with civil society organizations raising concerns over potential asset flight. Meanwhile, Mikhail Fridman secured permission to challenge a NCA's raid at his London property as part of another investigation into alleged sanction evasion, an "egregious" conduct in obtaining a search warrant, according to the judge (Fridman v. National Crime Agency, case number CO/760/2023).

Sanctions have not prevented designated parties from attempting to circumvent sanctions either. While cases of sanctions evasion have started to be brought before US courts, the UK's Combatting Kleptocracy Cell, specifically tasked with targeting evasion, is yet to showcase concrete results. Beyond the timid investigations into alleged misconduct by Aven and Fridman, being tougher on sanctions evasion remains in the UK a policy intention rather than a reality. Yet, there is evidence of designated individuals proactively restructuring their wealth to avoid detection, often shortly before sanctions hit.

To prevent this, in June 2023 the UK government announced its intention to introduce a disclosure obligation for designated persons under UK sanctions surrounding the assets they hold in the UK. This proposal, which was initially advanced by the Royal United Services Institute and Spotlight on Corruption, awaits publication – its impact on enhancing sanctions enforcement unknown.

SHIFTING PARADIGMS

Sanctions have traditionally served as a foreign policy instrument aimed at inducing behavioral change, with the expectation that, once achieved, they can be lifted. As Mr. Justice Garnham wrote in the *Shvidler* judgment, "the effects of a designation are temporary and reversible, not fixed and permanent". Recent developments in the UK sanctions landscape, however, denote a shift from conventional practices surrounding the interpretation and enforcement of sanctions designations.

A question then arises: what criteria must be met for sanctions to be lifted in the UK? The *Shvidler* case illustrates that merely speaking out against the war may not suffice, and sanctions can persist even if the designated individual has altered their behavior. Opting for an administrative route, rather than a litigious one, has proven to be more effective. For instance, Oleg Tinkov successfully persuaded the FCDO to lift sanctions through an out-of-court administrative review, on the grounds that he was no longer in a sector of strategic significant for the Russian economy. In this case, the role of the FCDO in making the decision, rather than the court's, was pivotal. For oligarchs seeking to have their name struck off the sanctions list, garnering support from the UK government appears to be key. Speculation has circulated about designated individuals voluntarily transferring part of their wealth for Ukraine's recovery and denouncing the Kremlin's actions in Ukraine in exchange for lifting sanctions – a proposal notably supported by Fridman himself. Together with the proposal to introduce disclosure obligations, the UK government announced in June 2023 new legislation that would allow sanctioned oligarchs to donate frozen funds to Ukraine for its reconstruction. Even though it has denied a direct link between this proposal and sanctions relief, questions arise surrounding its efficacy, which hinges on the incentives for oligarchs to come forward, and the importance of not skewing the purpose of sanctions in the process.

The latter discourse also brings back into the spotlight a matter that – albeit not present in UK courts yet – has been a topic of conversation since February 2022: the recovery of assets currently frozen under sanctions. On the one hand, the Government's announcement of disclosure obligations for sanctioned individuals may trigger the introduction of a "failure to disclose" offense as a form of sanctions evasion which could lead to confiscation of some assets, albeit in limited amount. On the other hand, the Government's emphasis on the voluntary nature of donations indicates an intention, at least in the asset recovery context, of ensuring fairness and proportionality, as the frozen assets of sanctioned individuals and entities cannot legitimately be seized in the absence of a specific criminal conduct. As other countries push for furthering measures that would allow confiscation stemming from a sanctions designation (see, for instance, Canada's Bill S-278, An Act to amend the Special Economic Measures Act (disposal of foreign state assets)), one may wonder how long this balance will be respected.

CONCLUSIONS

In the realm of UK sanctions, striking a balance between inducing behavioral change, ensuring fairness and proportionality, and seeking targeted legal action against criminal conduct is paramount. It is a crucial, yet complex, imperative which has emerged in 2022, manifested in 2023, and will continue to shape the dynamics of sanctions implementation in 2024.

Sanctions, while a useful policy tool, not only in the foreign policy realm but in the criminal justice context as well, should not be the default option when criminality is identified. While UK courts have so far demonstrated a disposition towards not putting themselves in the executive's shoes as relates to sanctions designation processes, they have also proven to be more cautious when criminal conduct - whether sanctions evasion or corruption – is involved. Once key concepts surrounding sanctions designations are established, the enforcement of sanctions in the UK context will need to take account of many factors, including the evolving legal landscape, challenges posed by designated entities and individuals, individual rights and rule of law challenges, and political imperatives.

AUTHOR

Maria Nizzero

Fellow Maria Nizzero is Research Fellow, Centre for Financial Crime & Security Studies, Royal United Services Institute.

Share This Read

The International Academy of Financial Crime Litigators Founders

For further information, please consult our website:
www.financialcrimelitigators.org

STÉPHANE BONIFASSI
Bonifassi Avocats

LINCOLN CAYLOR
Bennett Jones

ELIZABETH ORTEGA
ECO Strategic Communications