The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1368-5201.htm

Money laundering and sanctions enforcement: large rewards, leniency and witness protection for whistleblowers

Theo Nyreröd and Stelios Andreadakis
Brunel Law School, Brunel University, Uxbridge, UK, and
Giancarlo Spagnolo
Department of Economics, Stockholm University, Stockholm, Sweden, and Stockholm Institute of Transition Economics, Stockholm, Sweden

Received 26 May 2022
Revised 15 June 2022
Accepted 15 June 2022

Abstract

Purpose – With sanctions becoming an increasingly important tool in ostracising autocratic regimes from western markets, the need for effective enforcement of sanctions and anti-money laundering (AML) is increasing, and the global AML regime will be the backbone to detecting evasion of sanctions. This regime, however, has been widely criticised as ineffective. This paper aims to discuss issues with the current sanctions/AML regime and propose a reward scheme for whistleblowers to enable asset seizures that is not reliant on its effectiveness.

Design/methodology/approach – This paper reviews weaknesses in the global AML regime, provide suggestions on how to design whistleblower reward programmes, based on agency experience and empirical evidence, as well as elaborate on how to use such programmes in the AML context.

Findings – This study concludes that for reward programmes to be effective in the context of AML and sanctions enforcement, they need to include witness protection and leniency for money launderers, though not for those convicted of a criminal offence associated with the predicate crime. Moreover, rewards should be mandatory and scale with the amount of money seized or confiscated, and the cap on monetary rewards should be higher than it is under the Kleptocracy Asset Recovery Rewards Programme in the USA.

Originality/value – In contrast to how the USA went about implementing rewards in this area under the Kleptocracy Asset Recovery Rewards Programme, this study argues that these programmes should be designed differently. This study also provides novel advice to governments on different design dimensions in the AML context and a model with three crucial pillars along with other design dimensions that should be considered.

Keywords Rewards, Sanctions, Whistleblowers, Money laundering, Leniency, Witness protection

Paper type General review

1. Introduction

Russia's invasion of Ukraine has illustrated that a central deterrence tool for western democracies will be sanctions on individuals, assets seizures and banning certain exports and imports. Now it is aimed at Russia, but non-militaristic interventions of this kind are likely to be the future go-to response to aggression by autocratic regimes – as it already was with respect to Belarus and the annexation of Crimea in 2014. Sanctions, however, are only effective if it is difficult or costly to circumvent them.

Some are concerned that, while an initial shock because of unexpected sanctions may generate disruptions, a substantial part of prohibited goods can eventually be

Journal of Money Laundering Control
© Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-05-2022-0068

imported/exported through third-party intermediaries in non-sanctioned countries to limit the effectiveness of sanctions. False labelling of origin, misinvocing, etc., are all likely to occur in such a case and will be difficult to detect without insiders. Analogously, sanctioned individuals' assets may shift hands, be laundered through shell companies without known beneficial owners and eventually end up being used again somewhere in the west.

There is a large network of law firms, private detectives and PR firms that do the bidding of Russian oligarchs, particularly active in the UK, whose workings were outlined by Bill Browder, the Head of the Global Magnitsky Justice Campaign, in a Congressional testimony on the 6th of April 2022 (Browder, 2022a). These lawyers are paid up to $1,300 an hour to target and harass those who call out the corruption of the current Russian regime. Browder has suggested targeting these firms by cancelling visas to the USA and prohibiting firms facilitating this activity from doing business with the USA. In this paper, we suggest an opposite and perhaps counterintuitive, approach: provide these people close to sanction individuals substantial monetary reward for information leading to asset seizures.

To get an idea of whom such a programme would aim to incentivise, consider the following story. In a new book, Bill Browder describes how he was aided by Alexander Perepilichnyy, a financial adviser for those involved in the large tax theft in Russia involving of Hermitage Capital and the torture and death of Sergei Magnitsky. Perepilichnyy helped launder the money for those involved in the tax theft, but eventually fell out with those criminals and turned whistleblower when he provided bank statements to Browder that led to the freezing of $11mn related to this fraud (Browder, 2022b, p. 39). His information provided a "road-map" to even be able to start investigating where the illegally stolen assets had ended up. Perepilichnyy later died while jogging near London in 2012, which some believe was a murder in retaliation for blowing the whistle (Dyrekilde and Abild, 2020). A reward scheme would aim at people like Perepilichnyy; in other words, persons who are unrelated to the predicate offence and other persons involved in the infrastructure that facilitates money laundering (financial advisers, real estate agents, tax advisors, lawyers, etc.).

In this paper, we outline the current AML framework, highlight some of its problems and discuss a relatively cheap and hard-to-detect ways to escape sanctions. We review and consider the United States Treasury's Kleptocracy Asset Recovery Rewards Programme, which was launched on the 16th of March 2022 (US Treasury, 2022) and elaborate on how monetary incentives can be used in the fight against money laundering and sanctions violations.

The remainder of this paper is structured as follows. Section 2 outlines the global AML regime, while Section 3 reviews criticism of the regime. In Section 4, we illustrate the problem with the global AML regime by considering the issue of trade-based money laundering. Section 5 provides a background on monetary reward programmes; Section 6 considers how to design effective reward programmes in the AML/sanctions context; and Section 7 concludes.

2. Global anti-money laundering preventative regime

The global standard setter for AML is the financial action taskforce (FATF), which has since 1989 issued recommendations to countries on how to combat money laundering and terrorist financing. While it was initially focused on drug money, the regime has been successively expanded – notable occasions include after the 9/11 attacks when countering financing of terrorism (CFT) became an integral part of the regime, and now it has received increased attention again, as it will be an important tool to ensure sanctions against Russian oligarchs are effective. Since its inception, the AML regime has come to incorporate much

more than drug offences and now includes numerous crimes: from corruption and human trafficking to tax evasion and environmental crimes. EU Directive (2018/1673) stipulates 22 categories of criminal activities that constitute predicate offences. The scope of entities covered by the regime has also successively increased: from banks and financial institutions to casinos and antique dealers.

FATF is a membership-based organisation and currently has 39 members, including two regional organisations, the European Commission and the Gulf Co-Operation Council, thus representing most major financial centres at the international level. It has "soft-power" – the main tools it uses to ensure compliance is putting non-compliant countries on its blacklist of "non-cooperative countries or territories" or on its grey list of countries under "increased monitoring" (FATF, 2022). Non-compliant countries pose a substantially higher risk of money laundering, and this is a factor that FATF compliant states/institutions must take into consideration before choosing to do business with institutions from a non-compliant jurisdiction. To assess members' compliance with FATF recommendations, members carry out national risk assessments (NRAs) and are subjected to mutual evaluation reports (MERs).

The obligations on financial institutions and other covered entities are numerous. They must assess risks and conduct due diligence along various axis: the customer in question (is this person on a sanctions list/politically exposed person?), the nature of the jurisdiction (is it on the FATF's grey list?), the nature and structure of the business (cash-intensive business? use of shell companies?) as well as collect documents, such as copies of passport and certifications of residency. Then, each transaction also must be scrutinised in a similar fashion, and certain transactions over a monetary threshold are automatically reported to the financial intelligence unit (FIU). Compliance fulfils two main functions: financial institutions do not onboard customers that present high money laundering risk and suspicious customers/transactions within the bank are reported to the FIU. Only in the USA, the financial crimes enforcement network (FinCEN), which is responsible for receiving suspicious activity reports (SARs), obtained 1,426,741 such reports in 2021 from depository institutions alone (FinCEN, 2022). We call these rules governing financial institutions the "preventative," or "administrative," global AML framework or regime, and it can be characterised as follows:

- *First-order compliance*: member-states comply with the FATF recommendations. Compliance is ensured by FATF through grey/blacklisting, MERs and NRAs.
- *Second-order compliance*: financial and other institutions comply with the AML regulations in their country. Compliance is ensured by supervisory authorities through audits and administrative sanctions.
- *Policy objective*: convictions of money launderers/predicate offenceoffence perpetrators. Prosecutors, financial police and supervisory authorities obtain evidence from financial institutions (SARs) that is used to seise illegally gained assets. Money launderers are denied bank access in the first place.
- *The FATF hypothesis*: first and second-order compliance are sufficient for the achievement of the objectives of the policy regime, namely, to discover money laundering, provide evidence for prosecutions that allow asset seizures and ideally deter predicate offences.

Numerous scandals in the past couple of years have highlighted a lack of second-order compliance, particularly in Europe. In 2018, the Hungarian National Bank fined MagNet Bank 47 million forints; in 2017, the Central Bank of Ireland fined the Bank of Ireland

€3.1mn; again, in 2017, the UK Financial Conduct Authority (FCA) fined Deutsche Bank £163mn; in 2015, the FCA fined Barclays £72mn for inadequate AML controls related to a high-value transaction for politically exposed persons (Kirschenbaum and Véron, 2018). According to Violationtracker.org, since 2016, the USA has issued AML-related fines on eight occasions to banks with headquarters in European countries for an aggregate amount of $1.7bn. In Sweden, a country with nine million inhabitants, most of its largest banks have been fined for AML violations: Handelsbanken (SEK35mn) and Nordea (SEK 50mn) in 2015, SEB (SEK 1bn) and Swedbank (SEK 4bn) in 2019. In terms of scale, what has been called the largest money laundering scandal in history started to unravel in 2018, when it was discovered that around $230bn of suspicious funds had been transferred through Danske Bank's Estonian branch (McConnell, 2020). Official reports have also verified and lamented the compliance problem in the EU, including a 2020 report by the European Banking Authority that concluded that "In several cases, banks continued to be in breach of the same legal provision many years after a fine had first been imposed but were not challenged by the respective competent authority" (EBA, 2020).

Subsequently, the policy responses have almost exclusively focused on enhancing first and second-order compliance by increasing supervisory resources, cooperation between FIUs, the resources and power of FATF, an EU-wide supervisor and the like. European finance ministers have suggested a European supervisory mechanism for ML/FT (JPP, 2019), that should focus on particularly at-risk institutions and intervene when national competencies are inadequate. Unger (2020) stresses the need for a European supervisory body and suggests that the European Public Prosecutors Office, which currently investigates financial crimes against the EU budget but could have its responsibilities expanded. This European supervisor "should be an autonomous body, sufficiently staffed, and have direct powers of sanctioning. Supervision should concern all financial institutions. Non-financial institutions should be excluded, since they are too diverse" (Unger, 2020, p. 13). Kirschenbaum and Véron (2020) also argue that a new EU agency is needed that should have a direct AML supervision mandate, as "supervisor of supervisors" always acts too late. In 2020, the EU Commission also suggested that, in light of recent scandals, there are "compelling reasons for an EU body to be entrusted with direct AML/CFT supervisory tasks over certain obliged entities for which it could have exclusive or joint responsibility. This implies the ability to review the internal policies, procedures and controls as well as their effective implementation by supervised entities, along with reviewing documentation on transactions and customers." (European Commission, 2020, p. 8). On the 20th of July 2021, the European Commission published a proposal of a sixth AML Directive and proposed a new EU AML Authority (European Commission, 2021).

To enhance second-order compliance, others have called for whistleblower rewards to those who report non-compliance by covered institutions (Spagnolo and Nyreröd, 2021a, Scarcella, 2021), and the USA recently passed the Anti-Money Laundering Act of 2020 (AMLA), which provides for awards to whistleblowers who bring forward information about violations of the Bank Secrecy Act (BSA) that covers SARs and obligations on financial institutions. Nevertheless, these recent policy responses that squarely put the problem on first and second-order non-compliance may be obscuring more fundamental issues with the global AML regime. Contrary to the FATF hypothesis, first and second-order compliance may not be sufficient to achieve the policy objective to a desirable degree or at a reasonable cost. The next section outlines some concerns along these lines, starting with costs and then considering effectiveness.

3. Criticism of the anti-money laundering regime and the financial action taskforce hypothesis

[Costs] Governments. For mutual evaluation reports, the FATF sends several investigators to evaluate a country's compliance with FATF recommendations. These reports frequently exceed 200 pages and are jointly carried out by at least three experts, but in most cases many more. For Italy and Spain, it took 16 days of on-site visits by eight and ten evaluators, respectively, to complete the MERs (van Duyne *et al.*, 2018, p. 359). Forsman (2020; p. 30) notes that for Sweden's MER published in 2017: "Merely to enable the assessment of technical compliance, Swedish authorities wrote a 334-page document that was submitted to the FATF together with hundreds of translations of acts, ordinances, instructions, strategies, process descriptions, decisions, written communications, brochures and so on."

[Costs] Covered entities: Then, there are costs for financial institutions, most of which is spent on Know Your Customer (KYC) procedures and AML compliance management. Compliance Week (2015, p. 12) approximated that, in the next two to three years after their 2015 report, financial institutions globally would be spending more than $10bn for AML compliance controls. In reality, however, the increase in the costs has been even greater. Celent estimates that financial industry spending on AMLKYC compliance information technology (IT) and operations will reach $37.1bn globally in 2021 (Celent, 2021). As for the UK, AML compliance is costing UK financial institutions a staggering £28.7bn annually and is set to rise to £30bn by 2023 (LexisNexis, 2021).

[Costs/Effectiveness] SARs: administrative burden. A former head of Europol remarked that "95% of suspicious activity reports sent to the FIUs are junk" (SNS, 2019) and a report including interviews with past and present heads of financial intelligence units concluded that 80%–90% of suspicious reporting is of no immediate value to active law enforcement investigations (Maxwell and Artingstall, 2017). This can be attributed to many reasons, such as the banks not having sufficient information to confidently determine whether there is indeed something suspicious or not, as well as defensive filing.

[Effectiveness] Inability to document effectiveness. Several researchers focusing on policy effectiveness have been sceptical of the AML regime and many have called for better regulatory impact assessments (Koker, 2022). Pol (2020) offers a summary of the criticism the last decades, citing over 22 articles that have "identified gaps between the intentions and results of the modern anti-money laundering effort, including its core capacity to detect and prevent serious profit-motivated crime and terrorism" (Pol, 2020, p. 103). Some of these issues are deeply concerning and require more detailed analysis, but because of space restrictions we will not deal with them here.

[Effectiveness] Available estimates are disappointing. The most frequently cited estimate is that much less than 1%, probably around 0.2% of the proceeds of crime laundered via the financial system are seized and frozen (UNODC, 2011, p. 7). Considering that in 2021, global GDP amounted to about $94.93tn (IMF), it becomes easily understood that illicit financial flows and dirty money can significantly distort the world economy and hamper economic growth.

[Effectiveness] Sensitive to a few instances of non-compliance. Even if the regime obtains second-order compliance rates of 95%, we have seen how sensitive the system is to instances of non-compliance, such as Danske Estonia, where a relatively small branch transferred $230bn of suspicious money in the span of around seven years.

[Effectiveness] New methods of laundering. The AML framework has another defect in that it is slow to respond to new methods of laundering money, such as the use of digital currencies, crypto-assets, platforms and privacy coins that aim to obscure who sends and receives the currency as well as the amount transacted (Srivastava *et al.*, 2019, pp. 50–51).

Extending the preventative framework to something like cryptocurrency exchanges, for example, takes years in jurisdictions, such as the EU where a Directive is published and member states have two years to transpose it into national law (with many countries frequently not meeting that deadline). Cryptocurrencies are merely one example and, while these new high-risk areas draw a lot of attention, there are already well-established methods of money laundering that are difficult to detect. The next section considers one such method which illustrates some of the problems with the present AML regime.

4. Trade-based money laundering

As with many forms of economic crime, it is difficult to get an accurate view of how prevalent it is. Money laundering poses further challenges because it can occur through a variety of channels. The term is believed to originate from the period of prohibition in the USA in the 1920s and 1930s, when laundromats were used to disguise the origin of money obtained from criminal activities. But laundromats, hair salons, bars, car workshops, casinos or indeed potentially any business is just one small part of a much larger picture. More intricate and widely used methods are available that enable larger sums to be laundered. Today, beyond use of the financial system and moving cash in bulk across countries, trade-based money laundering (TBML) is one of the most popular methods and has been described as the "new frontier in international anti-money laundering enforcement" (Cassara, 2016). TBML can be carried out by undervaluing exports or over-valuing imports. Take an example from Zdanowicz (2009, p. 858):

> Assume a terrorist or criminal wants to launder $1mn to a foreign country. He would need to have a foreign exporter to collude on the transaction. The set of transactions used to launder the money would include:

- foreign exporter purchases 10,000 razor blades for $10 per blade. ($1,000);
- foreign exporter exports 10,000 razor blades to a domestic importer for $100 per razor blade. (Total Invoice $1,000,000);
- domestic importer receives 10,000 razor blades worth $1,000 but pays the foreign exporter $1,000,000; and
- Outcome: The domestic importer has moved $1mn to the foreign country less the $1,000 transactions cost of the razor blades.

There is evidence that this form of money laundering has increased in response to further regulation of financial institutions. De Boyrie *et al.* (2006) studied a broadening of money laundering policy in Switzerland in 1998 under the Federal Act on The Prevention of Money Laundering in the Financial Sector. This Act expanded the reach of Switzerland's Code of Conduct on due diligence to include not only banks but the whole financial sector. Controlling for various factors, they found that the amount of money moved from Switzerland to the USA increased substantially, from about $253mn per month to $628mn per month after the law was enacted. The amount of money moved as a percentage of the Swiss/US trade also increased significantly, suggesting that some money traditionally moved through the financial system was instead moved through trade.

Global financial integrity (GFI) has studied the extent of "trade misinvocing," i.e. when "importers and exporters deliberately falsify the declared value of goods on the invoices they submit to their customs authorities in order to illicitly transfer money across international borders, evade tax and/or customs duties, launder the proceeds of criminal activity, circumvent currency controls and hide profits in offshore bank accounts"

(GFI, 2021, p. 1). To identify potential trade misinvocing, GFI use data from the United Nations Comtrade database to estimate the "value gap" between countries. For instance, if Ecuador reported exporting $400mn worth of bananas to the USA in 2016, but the USA reported only having imported $375mn worth of bananas, the mismatch or value gap would be $25mn. In analysing 134 developing countries' trade with all global trading partners, GFI estimates the value gap at $1.6trn in 2018 (compared to $934bn in 2009).

One may think that TBML would be easy to detect by comparing import/export valuations and conducting risk-based audits of the importers/exporters. However, the use of sophisticated methods, such as multiple invoices for the same goods, falsely described goods and services and modest over/underreporting diversified across different goods, makes this difficult to detect within the context of global trade which was estimated at $28.5tn in 2021 (UNCTAD, 2022). Moreover, many actors that facilitate TBML are not covered by the AML framework. A senior financial crime expert has suggested including "firms transporting or arranging the transport of goods such as brokers, freight forwarders, and carriers" into the AML framework, and that this "huge expansion" will necessitate the inclusion of "new categories of non-financial companies that are currently not the least bit knowledgeable or concerned about AML/CFT safeguards" (Cassara, 2016, Chapter 11). While trade transparency is certainly a desirable long-term goal, not only to fight ML, but also to ensure customs and tax rules, there is a risk that expanding the AML framework will impose substantial costs and few verifiable benefits, as the previous section highlighted.

The problem with the current AML regime, even if ideally implemented, is that it adopts an armchair approach that cannot verify the numbers, books and actual beneficial owners without costly physical inspections of inventories and businesses. Obtaining that information in other ways, which would involve lower costs and less resources employed, would be the most desirable approach. How can money laundering be combated and sanctions enforced, without excessive reliance on the preventative AML regime? Initially, we need to take a step back away from the bureaucracy that has evolved around compliance with the existing global regime and assess its original objectives: to detect money laundering, seise assets and (ideally but unlikely) deter predicate offences. The administrative framework is merely a means to that end. How can high-quality information on predicate offence perpetrators attempting to launder money be obtained by enforcement agencies directly, with less reliance on second-order compliance? We will consider a method that is increasingly used in the USA and that was now expanded to the AML context: providing large rewards to whistleblowers.

5. Background on reward programmes

In recent years, we have seen an increase in the number of programmes that offer substantial rewards for whistleblower's information. These programmes have proven highly successful in the USA, primarily with respect to fraud against the government (False Claims Act, 1863), tax evasion (Tax Relief and Healthcare Act, 2006) and securities fraud (Dodd-Frank Act, 2010). Under these programmes rewards of millions of dollars are paid to individuals who bring agencies information on infringements. The securities and exchange commission (SEC) had as of September 2021 paid over $1bn in rewards to whistleblowers who reported infringements of securities laws (SEC, 2021). Under the tax programme, the internal revenue service (IRS) had as of 2020 paid out over $1bn in rewards to whistleblowers for their information on tax evasion (IRS, 2020). With respect to fraud against the government, the False Claims Act has a ten-year average of $515mn annually paid to whistleblowers. Under these programmes, whistleblowers typically receive between

10%–30% of the tax recovered (IRS), fines paid (SEC) or government money recovered (FCA).

These programmes have become an important part of law enforcement in several regulatory areas in the USA: the SEC and IRS now have their own whistleblower offices, dedicated to reviewing whistleblower claims and that also provide annual reports to Congress on the functioning of these programmes. Agency staff and attorneys have praised these programmes for their effectiveness, calling them one of the most important enforcement tools (Delery, 2014; White, 2013, 2015; SEC, 2016; p. 3, Kohn and Wilmoth, 2020; DoJ, 2020). More importantly, empirical evidence in recent years has shown that these whistleblower reward programmes are effective at detecting and deterring crimes in a cost-effective way (Dyck, 2010; Wiedman and Zhu, 2018; Raleigh, 2020; Leder-Luis, 2020; Dey *et al.*, 2021; Berger and Lee, 2022; Nyreröd and Spagnolo, 2021 for a review). Available cost-estimates of the False Claims Act suggest that it is highly cost beneficial, Meyer (2013) estimates costs to benefits to be 1/20 and Carson *et al.* (2008, p.369) estimate it to be between 1/14 and 1/52.

While the USA has been the main country experimenting with reward programmes, this method of eliciting information is becoming increasingly popular. In the UK, for example, HM Revenue and Customs has confirmed that they paid £290,250 to informants in 2018 and £473,000 in 2019 and the office of fair trading (OFT) – now called the competition and markets authority (CMA)- offers financial rewards of up to £100,000 (in exceptional circumstances) for information about cartel activity. In Germany, the then finance minister Olof Schulz authorised a payment of €2mn euro for a CD containing information on tax evaders (Reuters, 2021). More and more jurisdictions are also introducing reward programmes in different areas, including Brazil, Canada, Peru, Hungary, Lithuania, Montenegro, Slovakia, Ukraine, UK, Kenya, Malaysia, Republic of Korea, Pakistan, Philippines, Taiwan and Vietnam.

Rewards have been available in the US AML context under the Bank Secrecy Act, but, in contrast to the above-mentioned US programmes, these rewards were handed out entirely at the treasury's discretion and were capped at $150,000. There is little evidence that discretionary rewards in this lower range are effective at eliciting information (Spagnolo and Nyreröd, 2021b), particularly quality information from high-level employees. Perhaps because of this, AMLA 2021 replaced the $150,000 reward with a reward of up to 30% of the fines paid for BSA violations, bringing it more in line with the SEC and IRS programmes. The same bill also introduced the Kleptocracy Asset Recovery Rewards Act (henceforth Kleptocracy Act), under which whistleblowers can receive up to $5mn "for information leading to seizure, restraint, or forfeiture of assets linked to foreign government corruption" (US Treasury, 2022).

While the value of whistleblowers in the AML context has been recognised (Yeoh, 2014), our suggestion in the next section – to reward those aiding criminals laundering their money – may be somewhat controversial. To ease some of these concerns, it should be mentioned that the practice of incentivizing culpable persons is common: plea bargaining is one example, when guilty persons receive some leniency in return for information. But it is also common under whistleblower laws in the USA. When the False Claims Act was introduced in 1863 during the US civil war, the senator, who tabled the Bill, stated that it aimed at "'setting a rogue to catch a rogue,' which is the safest and most expeditious way I have ever discovered of bringing rogues to justice" (Howard, 1863). The goal was not to enable good Samaritans to report solely in the public interest, as it is typically the case under contemporary whistleblower protection laws, but to enhance information gathering from any source, regardless of the motivation for coming forward with that information.

This is also reflected in contemporary reward practices in the USA. In 2012, Bradley Birkenfeld received $104mn under the IRS reward programme, despite serving a jail sentence for his involvement in facilitating tax evasion. Under the US reward programmes, rewards are typically denied if the whistleblower "knowingly planned or initiated" the wrongdoing. While there is a discussion to what extent culpable whistleblowers should be rewarded (Pacella, 2015), the spirit and practice of many of these laws suggest that those rewarded can be culpable to some extent in the wrongdoing. Outside of the USA, we can turn to other areas where large incentives are offered to culpable entities. In the area of competition law or "antitrust," highly successful leniency programmes offer the first reporting cartel participant complete immunity from fines (that would otherwise often have been millions of euros). In the EU, the European Commission is responsible for large cross-border antitrust cases. Over the 2010–2017 period, 23 out of 25 cartel investigations were the result of leniency applications: only two of these investigations resulted from the commission's own detection work (ECA, 2020, p.18). Incentive regimes of this kind have proven highly effective, but how should they be designed in the AML context, in order not to be entirely reliant on the preventative AML regime?

6. Design of reward programmes in the anti-money laundering context

We propose the following model for a reward programme in the AML context, following the lines of the Kleptocracy Act but with some modification. It has three main pillars:

1. witness protection and possibly guaranteed asylum for non-nationals;
2. leniency for money laundering offences, but not for any other crime; such as participating in the predicate offence; and
3. large rewards that are paid after the seizure/confiscation.

The first pillar is witness protection and guaranteed asylum. The Kleptocracy Act [(e)(4)] stipulates that the identity of the recipient of a reward or of the members of the recipient's immediate family can be protected, if deemed necessary. This witness protection scheme aims at offering anonymity to whistleblowers and their families, if there are concerns that they might become victims of retaliation, harassment or mistreatment of any kind. This provision is in line with the system followed by the SEC for disclosures made under the Dodd–Frank Act (Rule 21 F-7) and serves as an additional mechanism to encourage and motivate potential whistleblowers who do not wish their identity to be made known. On some occasions, the person providing information that leads to asset seizures will not be a resident in the jurisdiction that has the authority to seise the assets. In such cases, asylum for non-residents should be considered mandatory.

The second pillar is leniency for participating individuals. The Kleptocracy Act [(f)(2)] provides that "if the claim for a reward is brought by an individual who the Secretary has a reasonable basis to believe knowingly planned, initiated, directly participated in, or facilitated the actions *that led to assets of a foreign state or governmental entity being stolen, misappropriated, or illegally diverted or to the payment of bribes or other foreign governmental corruption, the Secretary shall appropriately reduce, and may deny, such award*. If such individual is convicted of criminal conduct arising from the role described in the *preceding sentence*, the Secretary shall deny or may seek to recover any reward" (our italics). A strict interpretation of participation in crimes that "led to assets of a foreign state or governmental entity being stole, misappropriated, or illegally diverted" appears to be strictly related to the predicate offence of corruption and not to secondary crimes, such as money laundering. If a person aids in money laundering, without any involvement in the

predicate offence of corruption in this case, then there are no grounds to reduce or deny an award according to (f)(2). If our interpretation is correct, this non-barring is for a good reason. If a person that in any way knowingly transacts money originating from a predicate crime, that person would have no incentive to turn to authorities as they would immediately incriminate themselves as well as being denied a reward. Our suggestion is to offer leniency for any offense related to money laundering, but not for any other crimes.

The third pillar is large financial incentives. The Kleptocracy Act offers discretionary rewards and also aims to "return the stolen assets or proceeds to the country harmed by the acts of corruption" (Sec 2 (b)(2)). These incentives complement the above two mechanisms and aim at building stronger law enforcement and maximising the effectiveness of all resources available. The monetary reward is meant to provide the financial means to provide for the whistleblower's well-being and to avoid retribution. Despite the cap at $5mn (unless the Secretary of the Treasury personally authorises a greater reward), it sends a clear message that the US Government and its enforcement agencies value information provided by whistleblowers. It is also limited to payments totalling $25mn on a yearly basis, although the President may waive this limitation, if appropriate. This is likely to happen if the programme experiences the same success as the other US reward programmes.

Beyond these three pillars, there are several other aspects that need to be considered when designing a rewards regime. It can, for example, be broad: an indefinitely ongoing programme providing rewards to anyone who submits information that leads to seizure or forfeiture, regardless of the predicate offence. Alternatively, it can be narrow: restricted with respect to time/persons/sectors and only reward information leading to seizures or forfeitures related to specific persons/crimes (e.g. for information on sanctioned Russian oligarchs but not tax evasion).

In the USA, lawyers often play an essential role as intermediaries between whistleblowers and enforcement agencies. A lawyer-intermediary approach has the benefit of having lawyers involved who can screen claims and know the prosecutorial bar for asset seizures. Their involvement can speed up the process and reduce the administrative burden as a whole. At the same time, whistleblowers are provided with high-quality representation and this model also offers significant incentives for the legal profession, creating "private attorney generals", willing to join the fight against money laundering. In the USA, attorneys are actively competing to represent whistleblowers under the above-mentioned programmes. Having said this, it needs to be highlighted that at present there are only a few lawyers of this kind outside the USA, and it would take years until a system of private attorney generals is developed. In addition, legal fees can be substantial, and this would necessitate larger rewards; this is something that the US Government will need to monitor and act upon in the future if the $5mn cap remains. Finally, lawyers themselves can become targets of retaliation by predicate offence perpetrators, but this phenomenon is likely to be eradicated by the prevalence of a substantial body of private attorney generals with expertise and a track record of successful cases.

Another option is the establishment of a direct contact system, according to which whistleblowers turn directly to prosecutors and enforcement agencies with their information. This system bears great resemblance to the Dodd–Frank system, as whistleblowers can share their information with the SEC, but, if they wish to remain anonymous, they must be represented by an attorney (SEC, 2022). In this way, there will be an open channel of communication between potential whistleblowers and the authorities, which in turn can lead to a significant increase in the number of tips and disclosures made. It will also offer a cheaper option, as no attorney fees are required. Inevitably, lower rewards will be offered, because of the absence of attorney fees, but it can be argued that the number of prosecutions and successful cases is more important than the size of rewards offered. On the other hand,

such a system is not free from drawbacks. More specifically, it will allow the influx of a huge number of low-quality tips or tips not always supported by adequate evidence. Equally, it will undermine the creation of a specialised body of private enforcers because there will not be any incentives on the legal side to consider becoming private enforcers.

Rewards in the Kleptocracy Act also differ from the IRS, SEC and FCA programmes in two important ways. First, the rewards are discretionary, and secondly, they are capped at $5mn. This cap may be problematic as someone, who has knowledge of $3bn in corruptly gained assets, may not want to blow the whistle for $5mn, but would do so for $50mn. The model providing 10%–30% of recoveries, fines or seized assets has the benefit that the incentive to the whistleblower scales with the severity of the offence. To stay in line with agency experience and the empirical evidence, we therefore suggest a scaling reward model as well as mandatory rewards if the information is essential to the asset seizure. The following model is the one most supported by the evidence adjusted to suit the money laundering/sanctions enforcement context:

(1) leniency for money laundering offences, but not any other crimes;

(2) witness protection and guaranteed asylum;

(3) large mandatory rewards:
- 10%–15% under a direct-contact approach.
- 15%–30% under a lawyer-intermediary approach.
- Right to appeal a no-reward decision.

This merely provides a fundamental structure that can serve to guide the debate on reward programmes in the money laundering and sanctions enforcement context. Numerous other design dimensions must also be considered, such as adding a minimum threshold for rewards to be considered to reduce the number of low-value claims. Under Dodd–Frank, for example, that threshold is $2mn. If rewards under the Kleptocracy Act prove effective, then that model may be desirable for other countries as well.

7. Conclusions

The Russian aggression against Ukraine and the subsequent sanctions have put increased emphasis on the ability and effectiveness of the current AML regime to detect money laundering and sanction evasions by generating information leading to asset seizures. Justified concerns about this regime have been raised, and its performance record is still under question. We aim to provide a model of obtaining information leading to asset seizures that do not rely on the global AML regime and turn to whistleblower reward programmes that are becoming increasingly popular and have proven effective in numerous regulatory areas. In this paper, we have argued that countries that wish to enhance compliance should institute programmes that offer large mandatory rewards, witness protection and leniency for whistleblowers.

References

Berger, P. and Lee, H. (2022), “Did the Dodd-Frank whistleblower provision deter accounting fraud?”, *Journal of Accounting Research*, Early view, doi: 10.1111/1475-679X.12421.

Browder, B. (2022a), “Testimony to the US Helsinki commission: Countering oligarchs, enablers, and lawfare”, 6 April 2022, available at: www.csce.gov/sites/helsinkicommission.house.gov/files/Browder.pdf (accessed 19 May 2022).

Browder, B. (2022b), *Freezing Order*, Simon and Schuster, New York, NY.

Carson, T., Verdu, M. and Wokutch, R. (2008), "Whistle-blowing for profit: an ethical analysis of the federal false claims act", *Journal of Business Ethics*, Vol. 77 No. 3, pp. 361-376.

Cassara, J. (2016), *Trade Based Money Laundering: The Next Frontier in International Money Laundering Enforcement*, John Wiley and Sons, NJ.

Celent (2021), "IT and operational spending in AML-KYC: 2021 edition", Celent, 14 December 2021, available at: www.celent.com/insights/428901357 (accessed 19 May 2022).

Compliance Week (2015), "AML compliance: 2015 update", e-Book provided by KPMG, available at: www.complianceweek.com/download?ac=6013 (accessed 19 May 2022).

de Boyrie, M.E., Pak, S.J. and Zdanowicz, J. (2006), "The impact of Switzerland's money laundering law on capital flows through abnormal pricing in international trade", *Applied Financial Economics*, Vol. 15 No. 4, pp. 217-230.

Delery, S. (2014), "Assistant attorney general stuart delery delivers remarks at American bar association's 10th national institute on the civil false claims act and qui tam enforcement", *US Department of Justice Office of Public Affairs*, 5 June, available at: www.justice.gov/opa/speech/assistant-attorney-general-stuart-delery-delivers-remarks-american-bar-association-s-10th (accessed 19 May 2022).

Dey, A., Heese, J. and Pérez-Cavazos, G. (2021), "Cash-for-Information whistleblower programs: effects on whistleblowing and consequences for whistleblowers", *Journal of Accounting Research*, Vol. 59 No. 5, pp. 1689-1740.

DoJ (2020), "Justice department recovers over $3 billion from false claims act cases in fiscal year 2019", *US Department of Justice Office of Public Affairs*, 9 January, available at: www.justice.gov/opa/pr/justice-department-recovers-over-3-billion-false-claims-act-cases-fiscal-year-2019 (accessed 19 May 2022).

Dyck, A., Morse, A. and Zingales, L. (2010), "Who blows the whistle on corporate fraud?", *The Journal of Finance*, Vol. 65 No. 6, pp. 2213-2253.

Dyrekilde, B. and Abild, L. (2020), *Man of Power – A True Story about Bill Browder, Money Laundering and Media Manipulation*, Kontrovers, Stockholm, Sweden.

EBA (2020), "On competent authorities' approaches to the anti-Money laundering and countering the financing of terrorism supervision of banks", European Banking Authority (EBA), EBA/Rep/2020/06.

ECA (2020), "The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight", Special Report No 24, European Court of Auditors (ECA), available at: www.eca.europa.eu/en/Pages/DocItem.aspx?did=56835 (accessed 19 May 2022).

European Commission (2020), "Communication from the commission on an action plan for a comprehensive union policy on preventing money laundering and terrorist financing", *(7.5.2020), C(2020) 2800 Final*.

European Commission (2021), "Anti-money laundering and countering the financing of terrorism legislative package", available at: https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en (accessed 19 May 2022).

FATF (2022), "Jurisdictions under increased monitoring – march 2022", the Financial Action Taskforce (FATF), available at: www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-march-2022.html (accessed 19 May 2022).

FinCEN (2022), "SAR filings by industry", Financial Crimes Enforcement Network (FinCEN), available at: www.fincen.gov/reports/sar-stats/sar-filings-industry (accessed 19 May 2022).

Forsman, M. (2020), "30 Years of combating money laundering in Sweden and internationally – does the system function as intended?", *Sveriges Riksbank Economic Review*, Vol. 1, pp. 24-55.

GFI (2021), "Trade-Related illicit financial flows in 134 developing countries 2009-2018", Global Financial Integrity (GFI) 2021 report, available at: https://gfintegrity.org/report/trade-related-illicit-financial-flows-in-134-developing-countries-2009-2018/ (accessed 19 May 2022).

Howard, J.M. (1863), "Congressional globe", Senate, 37th Congress, 3rd Session, pp. 955-956.

IRS (2020), "Fiscal Year 2020 Annual Report, IRS Whistleblower Office" Internal Revenue Service (IRS), Office of the Whistleblower, available at: www.irs.gov/pub/irs-pdf/p5241.pdf (accessed 19 May 2022).

JPP (2019), "Joint position paper by the ministers of finance of France, Germany, Italy, Latvia, The Netherlands, and Spain", available at: https://zoek.officielebekendmakingen.nl/blg-910249.pdf (accessed 19 May 2022).

Kirschenbaum, J. and Véron, N. (2018), "A better European architecture to fight money laundering", Peterson Institute for International Economics, Policy Brief 18-25, 18, available at: www.piie.com/publications/policy-briefs/better-european-architecture-fight-money-laundering (accessed 19 May 2022).

Kirschenbaum, J. and Véron, N. (2020), "A european anti-Money laundering supervisor: from vision to legislation", *Peterson Institute for International Economics*, 24 January, available at: www.bruegel.org/2020/01/a-european-anti-money-laundering-supervisor-from-vision-to-legislation/ (accessed 19 May 2022).

Kohn, M. and Wilmoth, M.J. (2020), "The 100 whistleblowers who changed wall street", The National Law Review, 28 September, available at: www.natlawreview.com/article/100-whistleblowers-who-changed-wall-street (accessed 19 May 2022).

Koker, L.D. (2022), "Editorial: Regulatory impact assessment: towards a better approach for the FATF", *Journal of Money Laundering Control*, Vol. 25 No. 2, pp. 265-267.

Leder-Luis, J. (2020), "Whistleblowers, private enforcement, and medicare fraud", Working Paper, Massachusetts Institute of Technology, available at: https://sites.bu.edu/jetson/files/2020/07/False-Claims-Act-Paper.pdf (accessed 19 May 2022).

LexisNexis (2021), "Cutting the costs of AML compliance" LexisNexis Risk Solutions Report, available at: https://solutions.risk.lexisnexis.co.uk/cutting-the-costs-of-aml-compliance (accessed 19 May 2022).

McConnell, P. (2020), "Danske bank – a smorgasbord of risks", *Journal of Business Accounting and Finance Perspectives*, Vol. 2 No. 3, doi: 10.35995/jbafp2030017.

Maxwell, N. and Artingstall, D. (2017), "The role of financial Information-Sharing partnerships in the disruption of crime", *Royal United Services Institute for Defence and Security Studies (RUSI) Occasional Paper, 17 October*, available at: https://rusi.org/explore-our-research/publications/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime (accessed 19 May 2022).

Meyer, J. (2013), "Fighting medicare and medicaid fraud: the return on investment from false claims act partnerships", Taxpayers Against Fraud Education Fund, available at: www.taf.org/the-roi-from-fca-partnerships (accessed 19 May 2022).

Nyreröd, T. and Spagnolo, G. (2021), "Myths and numbers on whistleblower rewards", *Regulation and Governance*, Vol. 15 No. 1, pp. 82-97.

Pacella, J. (2015), "Bounties for bad behavior: rewarding culpable whistleblowers under the Dodd-Frank act and internal revenue code", *University of Pennsylvania Journal of Business Law*, Vol. 17 No. 2, pp. 345-392.

Pol, R. (2020), "Responses to money laundering scandal: evidence-informed or perception-driven?", *Journal of Money Laundering Control*, Vol. 23 No. 1, pp. 103-121.

Raleigh, J. (2020), "The deterrent effect of whistleblowing on insider trading", University of Minnesota Working Paper, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3672026 (accessed 19 May 2022).

Reuters (2021), "Germany buys Dubai data to track possible tax evasion", 7 June, available at: www.reuters.com/world/middle-east/germany-buys-dubai-data-track-possible-tax-evasion-2021-06-11/ (accessed 19 May 2022).

Scarcella, G. (2021), "Qui tam and the bank secrecy act: a Public-Private enforcement model to improve anti-Money laundering efforts", *Fordham Law Review*, Vol. 90 No. 3, pp. 1359-1395.

SEC (2016), "Annual report to congress on the Dodd-Frank whistleblower program", Securities and Exchange Commission (SEC) Office of the Whistleblower, available at: www.sec.gov/files/owb-annual-report-2016.pdf (accessed 19 May 2022).

SEC (2021), "SEC surpasses $1 billion in awards to whistleblowers with two awards totaling $114 million", Securities and Exchange Commission (SEC), available at: https://www.sec.gov/news/press-release/2021-177 (accessed 19 May 2022).

SEC (2022), "Form TCR: Tip, compliant or referral", securities and exchange commission (SEC)", available at: www.sec.gov/files/formtcr.pdf (accessed 19 May 2022).

SNS (2019), "SNS/SHOF finance panel: money laundering and the financial sector – talk with Europol's former head", Seminar at the Centre for Business and Policy Studies (SNS), 2 February, available at: www.sns.se/en/articles/sns-shof-finance-panel-money-laundering-and-the-financial-sector-talk-with-europols-former-head/ (accessed 19 May 2022).

Spagnolo, G. and Nyreröd, T. (2021a), "Money laundering and whistleblowers", report written for Centre for Business and Policy Studies (SNS), available at: https://snsse.cdn.triggerfish.cloud/uploads/2021/11/money-laundering-and-whistleblowers.pdf (accessed 19 May 2022).

Spagnolo, G. and Nyreröd, T. (2021b), "Financial incentives to whistleblowers: a short survey", Sokol, D. and van Rooij, B. (Ed.), *Cambridge Handbook of Compliance*, Cambridge University Press, Cambridge, pp. 341-351.

Srivastava, A., Simpson, M. and Powell, R. (2019), *International Guide to Money Laundering Law and Practice*, Bloomsbury Professional, London.

UNCTAD (2022), "Global trade hits record high of $28.5 trillion in 2021, but likely to be subdued in 2022", United Nations Conference on Trade and Development (UNCTAD), 17 February, available at: https://unctad.org/news/global-trade-hits-record-high-285-trillion-2021-likely-be-subdued-2022 (accessed 19 May 2022).

Unger, B. (2020), "Improving anti-Money laundering policy", Study requested by the ECON Committee, European Parliament, available at: www.europarl.europa.eu/RegData/etudes/STUD/2020/648789/IPOL_STU(2020)648789_EN.pdf (accessed 19 May 2022).

UNODC (2011), "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes", Research report, united nations office on drugs and crime, available at: www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf (accessed 19 May 2022).

US Treasury (2022), "U.S. Departments of treasury and justice launch multilateral russian oligarch task force", March 16, available at: https://home.treasury.gov/news/press-releases/jy0659 (accessed 19 May 2022).

van Duyne, P., Harvey, J. and Gelemerova, L. (2018), "A 'risky' risk approach: Proportionality in the ML/TF regulation", King, C., Walker, C. and Gurulé, J. (Eds), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Palgrave Macmillan, London, pp. 345-374.

White, M.J. (2013), "Remarks at the securities enforcement forum", Securities and Exchange Commission (SEC), 9 October, available at: www.sec.gov/news/speech/spch100913mjw (accessed 19 May 2022).

White, M.J. (2015), "The SEC as the whistleblower's advocate", Securities and Exchange Commission (SEC), 30 April, available at: www.sec.gov/news/speech/chair-white-remarks-at-garrett-institute.html (accessed 19 May 2022).

Wiedman, C. and Zhu, C. (2018), "*Do the SEC Whistleblower Provisions of Dodd-Frank Deter Aggressive Financial Reporting*?", *2018 Canadian Academic Accounting Association Annual Conference*, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3105521 (accessed 19 May 2022).

Yeoh, P. (2014), "Enhancing effectiveness of anti-Money laundering laws through whistleblowing", *Journal of Money Laundering Control*, Vol. 17 No. 3, pp. 327-342.

Zdanowicz, J.S. (2009), "Trade-Based money laundering and terrorist financing", *Review of Law and Economics*, Vol. 5 No. 2, pp. 855-878.

Corresponding author
Theo Nyreröd can be contacted at: theo.nyrerod@hotmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**