FINANCIAL CRIME BRIEF

PROLIFERATION FINANCING AND THE PRIVATE SECTOR

KEEPING PACE WITH REGULATORY EXPECTATIONS

ACUMINOR

PROLIFERATION FINANCING AND THE PRIVATE SECTOR: KEEPING PACE WITH REGULATORY EXPECTATIONS

As our UK audience is no doubt aware, the need to raise awareness and understanding of proliferation financing (PF) within the private sector has never been more urgent. It has been three years since FATF amended its Standards[1] to require that FIs[2] and DNFBPs[3] take sufficient steps to identify, assess and mitigate the PF risks to which their businesses may be exposed.[4] Those amendments were given legal force in the UK last year[5]: as of September 2022, regulated entities must conduct a PF risk assessment, and produce a copy to the relevant supervisory authority on request.[6]

As a global leader in counter-PF efforts, the UK is among the first to translate the amended Standards into domestic law – but other jurisdictions can certainly be expected to follow suit.[7] Even in the absence of legislative change, rising regulatory expectations may well render PF risk assessments a necessity in practice.[8] While institutional understanding of PF risk may be relatively nascent, and the regulatory guidance somewhat slim[9], experts have pointed to a number of factors that should be taken into account when assessing potential exposure. This paper provides a brief overview of the latest intelligence on the subject, highlighting some of the key indicators that may help inform assessments as to potential PF risk.

LIST OF ACRONYMS	
AML	Anti-money laundering
CDD	Customer due dilligence
CTF	Counter-terrorist financing
DNFBP	Designated non-financial businesses and professions
DPRK	Democratic People's Republic of Korea
FATF	Financial Action Task Force
FI	Financial Institution
KYC	'Know Your Customer'
MLR	Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
MVTS	Money or value transfer services
NRA	National Risk Assessment
PF	Proliferation Financing
TFS	Targeted financial sanctions
UNSC	United Nations Security Council
WMD	Weapons of mass destruction

UNDERSTANDING THE THREAT ENVIRONMENT

This month marks one year since the relevant amendments to the UK's MLR came into force.[10] Those amendments were expressly designed to align domestic legislation with the FATF standards, and ensure that the private sector takes sufficient steps to detect and prevent the potential breach or evasion of targeted financial sanctions (TFS).[11]

The underlying objective is, of course, not a novel one. Along with AML and CTF obligations, PF-related TFS have long formed part of the compliance landscape. Unlike AML and CTF, however, PF has not typically been viewed as a foundational aspect of the business-wide risk assessment, but rather subsumed within the broader sanctions 'bucket'. As articulated in the UK's first national risk assessment (NRA) on PF, the amended regulations represent a significant shift, elevating PF considerations to now form a key component of any robust compliance programme.[12] The distinction is an important one: though the UK's approach to PF-related TFS has previously been assessed as highly effective[13], understanding of sanctions obligations in the UK varies across industry[14], with uneven implementation among smaller banks, MVTS providers and DNFBPs.[15] The amended regulations thus seek to enhance that understanding – and, with it, compliance.[16]

Understanding and awareness gaps are of course not confined to the UK.[17] Indeed, as one expert has observed, compared with money laundering and terrorist financing, PF is both harder to detect and less understood.[18] The immediate question is thus one of definition: What is PF risk?

FATF STANDARDS

Under the FATF Standards, PF risk is narrowly scoped, referring "strictly and only to the potential breach, non-implementation or evasion" of TFS referred to in Recommendation 7.[19] For the purposes of R.7, the relevant TFS are those imposed by the United Nations Security Council (UNSC) pursuant to its resolutions regarding weapons of mass destruction (WMD), in relation to two country-specific regimes: the Democratic People's Republic of Korea (DPRK) and the Islamic Republic of Iran.[20]

BROADER PF RISKS

This qualified definition is not without its critics, with some commentators lamenting the "missed opportunity" to capture potential proliferators beyond those associated with the DPRK and Iran.[21] At a national level, however, it would seem the utility of a broader remit has not been overlooked. Several of the PF-centric NRAs to have emerged since 2020 contemplate a range of potential threat actors beyond the DPRK and Iran.[22] This widened lens carries important implications for the private sector.[23] As one expert recently cautioned, "for the purpose of their RAs, FIs should note that PF as defined by the FATF may not articulate the full range of financial activities that may support proliferation."[24]

In some jurisdictions – including the UK[25] – further guidance on the parameters of PF risk may be found in local legislation. In others, it remains a concept attended by greater ambiguity. In the absence of any international consensus, the definition established within the FATF Standards arguably serves as the minimum threshold for any institutional PF risk assessment.[26]

The DPRK: The most significant PF threat on a global scale

The DPRK currently represents the most significant PF threat on a global scale. Though it is the target of multiple sanctions regimes worldwide, Pyongyang persists in its efforts to advance its nuclear and missile weapons programme.[27] Those efforts accelerated in 2022, with the ballistic missile programme reaching "unprecedented intensity, diversity and operational capability".[28]

Sanctions have, by design, impeded the DPRK's access to global trade and financial services, severely limiting critical imports as well as the country's ability to raise revenue via legitimate means. The apparatus of the State is thus heavily supported through both illicit exports of coal – a primary source of income – and illicit imports of refined petroleum products, essential for the DPRK's military capabilities (as well as agriculture and infrastructure). Movements of smuggled cargo are facilitated through ship-to-ship transfers, with the DPRK having significantly increased its acquisition of vessels in 2022.[29]

Additional illicit revenue streams include the sale of military equipment[30]; the exploitation of overseas labour[31]; and malicious cyber activity, with a higher value of virtual assets stolen by DPRK actors in 2022 than in any previous year.[32]

Iran: In the wake of the Iran nuclear deal

Iran has long provoked international concerns regarding its nuclear ambitions. Though agreement was reached in 2015 that the country's nuclear activities would remain exclusively peaceful (the so-called 'Iran nuclear deal'[33]), implementation has faltered in recent years. Unlike the DPRK, Iran does not possess nuclear weapons; however, its stocks of enriched weapons-grade uranium are now believed to have reached more than 20 times the agreed limit[34], and the country continues to develop its ballistic missile capabilities.[35]

Although on a smaller scale compared to the DPRK, Iran relies on many of the same strategies and revenue streams to advance its nuclear weapons programme.[36] Oil and other petrochemical exports create significant income for the regime, while maritime links and networks of intermediary agents are relied upon to circumvent sanctions and procure controlled/dual-use goods on the international market.[37] Iran also raises funds through the mining of virtual currencies.[38]

RISK INDICATORS – WHERE SANCTIONS SCREENING AND KYC/CDD CONVERGE

Though there is a dearth of public enforcement actions in relation to PF[39], this is not indicative of untroubled waters.[40] PF activity is both clandestine and complex, and notoriously difficult to identify. Those challenges are widely acknowledged – indeed, FATF has explicitly rejected a 'zero-failure' approach to PF mitigation, recognising that even a robust compliance function may fail.[41] Such pragmatism does not, however, give grounds for complacency. It remains incumbent on the private sector to ensure that PF risk is both understood and minimised.

Critically, this is an exercise that necessarily extends beyond sanctions screening and the question of whether a customer or transaction generates a match. To that end, FATF[42], regulatory[43], industry[44] and other expert guidance[45] has highlighted a number of indicators that may be relevant when assessing potential exposure to PF risk. Some have a specific nexus to particular PF threats, while others are of broad application. Moreover, many extend beyond PF, and are already associated with existing ML and TF threats. That overlap is unsurprising, given that the same vulnerabilities that give rise to ML and TF can also be leveraged by proliferators.[46]

Reliance on the global commercial supply chain – and the fact that most cargo is moved by sea[47] – means that the maritime sector is particularly exposed to PF activity. Correspondent banking and trade finance play an integral role in facilitating such transactions, rendering both similarly vulnerable to exploitation. Much of the difficulty in identifying PF activity, however, arises from the fact that it frequently resembles legitimate trade.[48] Efforts at weeding out proliferators thus demand a more rigorous understanding of the customer profile and the transactions in which they can be expected to engage.[49]

'Red flags' commonly (but not exclusively) associated with PF activity are set out below. These represent just a fraction of the risk indicators that have been distilled from the intelligence available.

Transaction deals with dual-use goods or other controlled commodities

Rather than buying off-the-shelf weapons, proliferation networks are more likely to procure individual goods and component parts – transactions which may appear innocuous to those involved in the supply chain as well as those processing payments.[50] The challenges in recognising the potential proliferation purpose of an ostensibly commercial transaction are well documented.[51] However, FIs and DNFBPs should nonetheless be cognisant of the risk that such dual-use goods present.

Corporate customer is a shell or front company

Proliferation networks commonly operate through shell and front companies, shielding their identities behind corporate vehicles registered in jurisdictions not targeted by sanctions. The DPRK, for example, capitalises on the marine industry's complex ownership and operator arrangements to obscure the involvement of designated entities.[52] Even when discovered (and designated), the actors behind such vehicles often operate under new corporate identities within six to 12 months of designation[53] (though often retain the same addresses, phone numbers or managers[54]).

Corporate customer is involved in business events that do not match the business description/profile

To avoid unwelcome scrutiny, proliferators rely on a façade of innocuity, "hiding in plain sight amid a larger global ocean of small and medium enterprises".[55] Purportedly legitimate commercial activities disclosed at onboarding may thus not necessarily align with subsequent activity.

"EFFORTS AT WEEDING OUT PROLIFERATORS DEMAND A MORE RIGOROUS UNDERSTANDING OF THE CUSTOMER PROFILE AND THE TRANSACTIONS IN WHICH THEY CAN BE EXPECTED TO ENGAGE."

Transaction or goods are sent through another jurisdiction without any apparent commercial reason

While transshipment is both a common and legitimate aspect of global logistics, the volume of traffic through such hubs poses special risks regarding the diversion of proliferation-sensitive cargo. Third-party intermediaries or transshipment points are routinely used to circumvent sanctions and export controls, and obscure the ultimate destination of goods.

Parties involved in the trade transaction are controlled by the same individual(s)

A pattern associated with Iran's illicit procurement is the use of multiple companies located in differing jurisdictions under the control of a common owner.[56] A recent case between OFAC and a US-manufacturer provides an illustrative example. The UAE-incorporated subsidiary purchased commercial building materials from its US-based parent, falsely stating that the goods were for general inventory at the company warehouse in Dubai. Once arrived in the UAE, the US-origin goods were comingled with goods produced in Dubai and falsely relabelled as being of UAE-origin before being exported to Iran.[57]

The evasive tactics employed by proliferators reiterate the insufficiency of relying on sanctions screening alone, given that PF activity frequently involves actors well beyond those found on any sanctions list.[58] This reinforces the need to 'know' one's customer, and interrogate those transactions that are unusual or out-of-pattern, or which appear to have no sensible business rationale given the parties or jurisdictions involved. While no single indicator is conclusive of PF activity, each may warrant additional scrutiny when assessing the risk in relation to a particular customer, product or transaction.

CONCLUSION

The private sector has a critical role to play in ensuring that its activities do not erode the integrity of sanctions programmes and the policy objectives that underpin them. Access to financial services is vital to the advancement of proliferation ambition. Disrupting that access is thus essential to global efforts seeking to stymie the production of WMD.

Larger institutions may be exposed to PF activity given the services they offer and the volume and complexity of transactions they handle. On the other hand, smaller institutions may be vulnerable due to relative (or perceived) weaknesses in their compliance regimes. No matter the size, the regulatory and reputational consequences that may attend a breach of TFS can be severe. In addition to sanctions screening, effective PF mitigation necessarily turns on the quality of KYC and customer due diligence processes, as well as an understanding of the risks inherent to a particular product, transaction, industry or jurisdiction. Prior to the 2020 amendments, only a limited number of private sector firms had completed a PF risk assessment.[59] It is hoped many more will now take up the mantle.

REACH OUT TO THE AUTHOR

STEPHANIE YGOA
Intelligence Analyst at Acuminor
stephanie@acuminor.com

Read more about Acuminor here

SOURCES:

[1] FATF (2012-2023), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html ('FATF Standards').

[2] Financial institutions, defined in FATF Standards to include any natural or legal person whose business activities/operations include, *inter alia*, acceptance of deposits and other repayable funds from the public; lending; financial leasing; money or value transfer services; issuing and managing means of payment; financial guarantees and commitments; individual and collective portfolio management; and/or money and currency changing (see definition for full list of relevant activities/operations): FATF Standards, p 127.

[3] Designated non-financial businesses and professions, defined in FATF Standards to include: casinos; real estate agents; dealers in precious metals; dealers in precious stones; lawyers, notaries, other independent legal professionals and accountants; and trust and company service providers: FATF Standards, p 124.

[4] FATF Standards, Recommendation 1.

[5] Via regulation 6 of the Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 ('the MLR Amendment Regulations').

[6] That requirement is now reflected in regulation 18A of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR). Entities to which regulation 18A apply – or 'relevant persons' – include: credit institutions; financial institutions; auditors, insolvency practitioners, external accountants and tax advisers; independent legal professionals; trust or company service providers; estate and letting agents; high value dealers; casinos; art market participants; cryptoasset exchange providers; and custodian wallet providers: MLR, regulation 8.

[7] Even prior to the 2020 amendments, national risk assessments in relation to PF had already emerged across five jurisdictions (Cayman Islands, Gibraltar, Latvia, Portugal and the United States): see FATF (2021), *Guidance on Proliferation Financing Risk Assessment and Mitigation*, FATF, Paris, France, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Financingofproliferation/Proliferation-financing-risk-assessment-mitigation.html

[8] US authorities, for example, have signalled that there will be increased investment to address the 'troubling trend' that has emerged in what the Department of Justice describes as "the intersection of corporate crime and national security": Deputy Attorney General Lisa Monaco (2023, March 2). *Remarks at American Bar Association National Institute on White Collar Crime* [Speech]. Miami, FL, United States. https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national

[9] As one expert contends, a lack of DNFBP-specific guidance has produced awareness gaps that increase those sectors' vulnerability to PF risk in relation to the DPRK: see Erskine, S. (2022, January). *North Korean Proliferation Financing and Designated Non-Financial Businesses and Professions*. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/271_EI_DNFBPs_Final_0.pdf. See also Kassenova, T. and Early, B. (2023, July). *Countering the Challenges of Proliferation Financing*. The Center for Policy Research, University at Albany. https://www.albany.edu/rockefeller/news/2023-countering-challenges-proliferation-financing. The authors there point out that most government guidance to date is limited to implementing TFS, whereas the private sector needs guidance and training on conducting a PF risk assessment as well as on how they can incorporate a PF component in their KYC and transaction monitoring: see pp 33-34.

[10] Regulation 1(5) of the MLR Amendment Regulations.

[11] HM Treasury. (2022). *Explanatory Memorandum to the Money Laundering and Terrorist Financing (Amendment) (No. 2)* Regulations 2022, p 4. https://www.legislation.gov.uk/uksi/2022/860/pdfs/uksiem_20220860_en.pdf

[12] HM Treasury. (2021). *National risk assessment of proliferation financing*, p 4. https://www.gov.uk/government/publications/national-risk-assessment-of-proliferation-financing ('the UK PF-NRA').

[13] See FATF (2018), *Anti-money laundering and counter-terrorist financing measures – United Kingdom*, Fourth Round Mutual Evaluation Report, FATF, Paris http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html

[14] Ibid, p 108. See also the UK PF-NRA, supra n 12 at p 28, which observes that awareness of proliferation procurement methodologies is lacking in elements of the industrial sector, and across the UK economy more broadly.

[15] FATF, *supra* n 13 at p 87.

[16] HM Treasury. (2022, 14 July). *The Money Laundering and Terrorist Financing (Amendment) (No. 2) Regulations 2022 Statutory Instrument (Regulatory Impact Assessment),* pp 30 and 32. https://www.legislation.gov.uk/ukia/2022/70/pdfs/ukia_20220070_en.pdf

[17] FATF guidance apprehends those gaps on a global scale, observing generally that "risks increase when a financial institution, DNFBP or VASP does not understand the risks of potential sanctions evasion schemes and how to implement tailored, risk-based measures to mitigate those risks": FATF, *supra* n 7 at p 39.

[18] Kassenova, T. (2018). Challenges With Implementing Proliferation Financing Controls: How Export Controls Can Help. *World ECR: The Journal of Export Controls and Sanctions.*
https://carnegieendowment.org/2018/05/30/challenges-with-implementing-proliferation-financing-controls-how-export-controls-can-help-pub-76476

[19] FATF Standards, Recommendation 1 (supra *n 1).*

[20] FATF Standards, Recommendation 7 and its Interpretive Note (*supra* n 1).

[21] See Kassenova and Early, *supra* n 9 at p 12, arguing that the current approach "is a missed opportunity to encourage countries to develop and implement broader proliferation financing controls". 4.

[22] See, e.g., AUSTRAC. (2022). *Proliferation Financing in Australia: National Risk Assessment.* https://www.austrac.gov.au/sites/default/files/2022-12/AUSTRAC_Proliferation_Financing_in_Australia-National_Risk_%20Assessment_Web.pdf ('the Australian PF-NRA'), which explicitly goes beyond the requirements of Recommendation 1 and assesses exposure to a wide range of direct and indirect PF threats. See also Department of the Treasury. (2022). *National Proliferation Financing Risk Assessment.* https://home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf ('the US PF-NRA'), which notes increasing concern regarding Chinese and Russian military modernisation, and includes reference to PF risk associated with even non-state sponsored actors. Finally, the UK PF-NRA (supra n 12) includes its autonomous sanctions regime on chemical weapons as a PF threat distinct from that posed by the DPRK or Iran, and cautions against overlooking the role played by other states in global PF, such as China. The Czech Republic has also reportedly adopted a methodological framework to assess not only PF risk as defined under the FATF Standards, but also risks in relation to WMD or dual-use items in general, pursuant to relevant UNSC resolutions: see Newsroom SRSP. (2022, March 8). Czech Republic launches the Proliferation Financing National Risk Assessment. *Council of Europe*. https://www.coe.int/en/web/corruption/-/czech-republic-launches-the-proliferation-financing-national-risk-assessment. See also Newsroom SRSP. (2022, June 9). Raising awareness on proliferation financing risks among the private sector representatives in the Czech Republic. *Council of Europe*. https://www.coe.int/en/web/corruption/-/raising-awareness-on-proliferation-financing-risks-among-the-private-sector-representatives-in-the-czech-republic

[23] In calibrating their own risk matrices, regulated entities are typically expected to take account of risk assessments and other guidance published on a national level.

[24] També, N. (2023, June). *Institutional Proliferation Finance Risk Assessment Guide*. Royal United Services Institute for Defence and Security Studies, p 6. https://static.rusi.org/proliferation-finance-risk-assessment-special-resource.pdf

[25]For the purposes of the MLR, "proliferation financing" means: *the act of providing funds or financial services for use, in whole or in part, in the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling of, or otherwise in connection with the possession or use of, chemical, biological, radiological or nuclear weapons, including the provision of funds or financial services in connection with the means of delivery of such weapons and other CBRN-related goods and technology, in contravention of a relevant financial sanctions obligation*: regulation 16A(9). Relatedly, "relevant financial sanctions obligation" means a prohibition or requirement in regulations made under section 1 of the Sanctions and Anti-Money Laundering Act 2018 and imposed for one or more of the purposes in section 3(1) or (2) of that Act so far as it relates to compliance with a relevant UN obligation: MLR, regulation 16A(10).

[26] This is, of course, subject to local legal requirements. Countries are not precluded from requiring regulated entities operating in their respective jurisdictions to consider broader PF risks beyond those associated with the DPRK and Iran. Even if domestic legislation is silent as to potential broader PF threats, those risks should not be automatically discounted.

[27] The DPRK's activities in this regard are detailed in the 7 March 2023 Final Report of the Panel of Experts assisting the 1718 DPRK Sanctions Committee (Publication No. S/2023/171).https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2023_171.pdf

[28] *Ibid* at p 11.

[29] *Ibid* at p 4.

[30] Kassenova and Early, supra n 9 at p 25.

[31] *Ibid* at pp 25-26.

[32] Final Report of the Panel of Experts, *supra* n 27 at p 4.

[33]Joint Comprehensive Plan of Action (JCPOA), reached by Iran and the P5+1 countries (China, France, Germany, Russia, the UK and the US) in July 2015.

[34] United Nations. (2023, July 6). Iran nuclear deal: Despite differences, still 'best available option', Security Council hears. *UN News*. https://news.un.org/en/story/2023/07/1138432

[35] *Ibid*. As noted in the article, there are "divergent views" as to whether Iran's recent activities are inconsistent with the JCPOA.

[36] UK PF-NRA, supra n 12 at p 21.

[37] As the UK PF-NRA explains (supra n 12 at p 9): *Dual-use items are goods, software, technology, documents and diagrams which can be used for both civil and military applications. They can range from raw materials to components and complete systems, such as aluminium alloys, bearings, or lasers. They could also be items used in the production or development of military goods, such as machine tools, chemical manufacturing equipment and computers*.

[38] UK PF-NRA, supra n 12 at p 26.

[39] Enforcement action taken in the US is a notable exception.

[40] As Kassenova and Early observe, lack of WMD-related cases is a product of prosecutors' lack of awareness and experience (supra n 9 at p 38).

[41] FATF, *supra* n 7 at p 39.

[42] Ibid at pp 17-21; and FATF (2018), *Guidance on Counter Proliferation Financing – The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction*, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-counter-proliferation-financing.html , pp 32-34.

[43] See, e.g., the the UK PF-NRA (*supra* n 12), the US PF-NFRA and the Australian PF-NRA (supra n 22).

[44] See, e.g., International Chamber of Commerce. (2019). *How Does Global Trade and Receivables Finance Mitigate against Proliferation Financing*? (Policy Statement 470/1284). https://iccwbo.uk/products/icc-global-trade-receivables?_pos=1&_sid=dc9176676&_ss=r

[45] See, e.g., També, supra n 24; Brewer, J. (2018). *The Financing of Nuclear and Other Weapons of Mass Destruction Proliferation*. Center for a New American Security. https://www.cnas.org/publications/reports/the-financing-of-nuclear-and-other-weapons-of-mass-destruction-proliferation; Brewer, J. (2018). *The Financing of WMD Proliferation: Conducting Risk Assessments*. Center for a New American Security. https://www.cnas.org/publications/reports/the-financing-of-wmd-proliferation; and Brewer, J. (2017). *Study of Typologies of Financing of WMD Financing: Final Report. King's College London*. https://www.kcl.ac.uk/news/final-report-typologies-of-proliferation-finance

[46] També, *supra* n 24 at p 10.

[47] According to the United Nations Conference on Trade and Development, ships deliver over 80% of world trade: UNCTAD. (2022). *Review of Maritime Transport 2022: Navigating stormy waters*. https://unctad.org/rmt2022. The UK PF-NRA notes that 95% of all UK imports and exports are moved by sea: *supra* n 12 at p 23.

[48] US PF-NRA, *supra* n 22, p 17.

[49] See, e.g., recent comments of the UK's Financial Conduct Authority, stating its concern that the 'low' quality of KYC and CDD assessments has led to increased risk of firms not being able to identify sanctioned individuals: FCA. (2023, Sept 6). *Sanctions systems and controls: firms' response to increased sanctions due to Russia's invasion of Ukraine*. https://www.fca.org.uk/publications/good-and-poor-practice/sanctions-systems-and-controls-firms-response-increased-sanctions-due-russias-invasion-ukraine

[50] ICC, *supra* n 44 at pp 5-6.

[51] See ICC, *supra* n 44; and ICC. (2023). Financial crime risk controls – Dual-use goods and proliferation financing. https://iccwbo.org/wp-content/uploads/sites/3/2019/06/2023-ICC-Financial-crime-risk-controls-Dual-use-goods-and-proliferation-financing.pdf

[52] Final Report of the Panel of Experts, *supra* n 27 at p 288 (Annex 39).

[53] ICC, *supra* n 44 at p 4, citing 2018: RUSI and Dechert LLP Roundtable event: Supply Chain Risk and DPRK Sanctions.

[54] Kassenova and Early, *supra* n 9 at p 35.

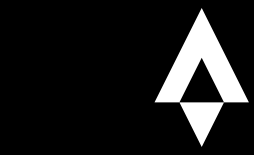
[55] US PF-NRA, *supra* n 22 at p 17.

[56] Kassenova and Early, *supra* n 9 at pp 28-29.

[57] Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Construction Specialties Inc. on behalf of itself and its subsidiaries and affiliates worldwide, including Construction Specialties, Middle East L.L.C (27 June 2023) https://ofac.treasury.gov/media/932091/download?inline

[58] ICC, *supra* n 44 at p 5. See also FATF, *supra* n 7 p 39.

[59] FATF, *supra* n 7 at p 11.



ACUMINOR

A BRIGHTER WORLD

Proliferation Financing and the Private Sector: Keeping Pace with Regulatory Expectations

Sveavägen 140
113 50 Stockholm
SWEDEN

1 Poultry
London EC2R 8EJ
UNITED KINGDOM

acuminor.com
+46 8 121 586 30
relations@acuminor.com