Member Circular No. 12/2021 February 2022

Sanctions – recent deceptive practices

Introduction
Since 2010, considerable sanctions' activity has been directed at shipping and its supporting industries reflecting the fact that 90% of world trade involves the carriage of goods by sea.

The purpose of this Circular is to draw Members' attention to some of the recent deceptive practices employed by parties that are engaged in activities that offend the sanctions regimes operated by national governments and or supranational bodies such as the UN.

Current deceptive practices observed by the International Group and its commercial partners
Whilst trade sanctions are applied widely by governments to promote individual foreign policy objectives, the following jurisdictions are particularly relevant in the context of controlled activities in maritime trade:

- Iran
- Syria
- Venezuela
- Democratic Republic of Korea (DPRK)
- Crimea
- Cuba

Cargoes traded in breach of international and national trade sanctions appear to be on the increase. Iranian oil exports, initially heavily restricted by sanctions programmes are now thought to have risen from an estimated 340,000 barrels per day in following the US withdrawal from the JCPOA to an estimated 1.3 million barrels per day in March 2021.[1] In recent weeks oil swap deals involving Iranian and Venezuelan oil cargoes destined for Asian markets have been widely reported in the press.[2] In September 2021 the United Nations Security Council Panel of Experts on DPRK published an interim report detailing widespread infringements of UN sanctions involving shipping and the DPRK.

Some of the techniques used to break sanctions have been in use for several years, while others are newer and have become more prevalent in the last 18 months. All aim to minimise surveillance and detection through confusion or concealment of the identities of vessels, their cargo, geographical location, and navigational activities. Such concealment poses risks for shipowners and their commercial partners who may inadvertently be employed to transport a sanctioned cargo.

These techniques include:

- Manipulating a vessel's Automatic Identification Signal (AIS) to disguise the vessel's location and / or to alter a vessel's digital identity.
- Changing a vessel's physical appearance.
- Falsifying vessel and / or cargo documentation.
- Multiple ship-to-ship cargo transfers to hide the fact that the cargo originated in a country to which a sanctions regime applies.

[1] Iran Sanctions. Congressional Research Service. https://crsreports.congress.gov RS20871
[2] "Under US sanctions, Iran, Venezuela strike oil export deal". Reuters 25 September 2021

Gard AS, P.O. Box 789 Stoa, NO-4809 Arendal, Norway Tel: +47 37 01 91 00, Fax: +47 37 02 48 10,
Outside office hours: +47 90 52 41 00

All these practices present risks for ship owners who without a properly implemented compliance framework may find that their vessel is being used to transport sanctioned cargoes.

AIS manipulation

Considerable emphasis is placed by UN reports and the US and UK maritime advisories[3] on the need to monitor the AIS transmissions of vessels as part of a properly implemented compliance framework.

However, AIS technology and its associated hardware and software were not designed for this purpose; the purpose of AIS was to identify ships in coastal areas and minimise the risk of a collision. Since its function was to promote safety, it was not designed to prevent the signal it transmits from being manipulated and it remains lawful to switch the transmission off in the interests of vessel safety and security.[4]

The ability to manipulate or simply turn off the signal leaves AIS vulnerable to exploitation by those breaking sanctions. Although AIS transponders have built-in security features to prevent them from transmitting falsified data, these features are inconsistent across manufacturers and can be circumvented. Depending on the model, the encoded details can be changed using passcodes that are not always well-protected.

In addition to directly tampering with the transmitter, a user can also purchase multiple AIS transponders and so create multiple digital AIS identities from a single vessel. Identity tampering and vessels disguising themselves physically and digitally is increasingly common.

Current techniques include:

1. *Switching off the AIS.*

Whilst switching off of an AIS transponder is permitted in certain circumstances by SOLAS, vessels engaged in sanctions breaking can also switch off their transponders to hide their position and movements. This practice remains common for less sophisticated sanction breakers who rely on legitimate excuses as to why a Master might choose to turn off the AIS transmitter and the fact that even a properly transmitted signal might not always be received.

Members engaging in STS operations are therefore advised to monitor the providing vessel's AIS updates for gaps in transmission records. This can be achieved through an AIS monitoring platform or service provided by commercial companies where additional context and algorithms are used to assess whether an unlawful activity may have occurred during gaps in AIS transmission.

In simple cases, operators may attempt to evade sanctions by switching off AIS transponders when, for example, entering the Gulf of Oman and switching it back on after loading or conducting an STS of

[3] To assist industry in their due diligence programmes, the US Department of State, the US Department of the Treasury's Office of Foreign Assets Control (OFAC), and the US Coast Guard published a Global Maritime Sanctions Advisory in May 2020, which provided compliance guidance to a range of marine-related sectors including shipowners, Flag Registries, Classification Societies, banks and insurance companies. In July the same year, the UK followed suit with the publication by the Office of Financial Sanctions Implementation of its own Maritime Guidance to assist entities and individuals operating within the UK maritime shipping sector to better understand their compliance obligations. Both publications emphasised the importance of a comprehensive sanctions' compliance programme properly integrated into a business's operational practices.

[4] Regulation V/19 of the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, requires all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and passenger ships irrespective of size to be fitted with an automatic identification system (AIS), as specified in SOLAS regulation V/19.2.4. See paragraph 21 of IMO Resolution A.917(22) which describes the circumstances when AIS may be disengaged - . A 917 22 (imo.org) . SOLAS V/34-1 *"The owner, the charterer, the company operating the ship as defined in Regulation IX/1, or any other person shall not prevent or restrict the master of the ship from taking or executing any decision which, in the master's professional judgement, is necessary for safety of life at sea and protection of the marine environment."*

a sanctioned cargo. More sophisticated entities may create false journeys prior to switching off AIS, to disguise a vessel's true course.

2. GPS/GNSS manipulation (position spoofing).
Some sanctions breakers now falsify the position a vessel broadcasts via its AIS, to disguise the true location of the vessel.

The most rudimentary instances of GPS/GNSS (global navigation satellite system) spoofing simply produce repeat AIS updates in a single location. More sophisticated examples can produce very realistic signals and can only be identified through comparison with additional independent data such as satellite imagery, physical sighting of the vessel, or synthetic aperture radar (SAR) tracks. The IG is concerned that there is an increasing use of GPS/GNSS spoofing to hide the true location of vessels breaking sanctions.

Members may wish to partner with an AIS monitoring platform expert capable of assessing the datasets needed to validate a vessel's true location.

3. AIS misuse
AIS transmissions are being increasingly used to replicate another vessel's identity. Vessels may transmit an MMSI (maritime mobile service identity) number known to be used by other vessels. As multiple vessels are broadcasting with these numbers, a sanction breaking vessel can "hide" in the noise created by the additional AIS updates or, when replicating another vessel's identity (becoming its "ghost" or "twin") exploit that other vessel's non-sanctioned status or activity.
The vessel whose identity is ghosted may be an innocent vessel selected at random, or it may be complicit in the sanctions breaking activity handing over its identity at a pre-arranged meeting at sea with the sanctions breaking vessel that then resumes AIS transmissions.

Identity tampering
Increasingly sophisticated techniques are being used by sanctions breakers to disguise the identity of a vessel.

1. Physically altering a vessel's appearance.
Satellite imagery and other surveillance techniques are used by civil and military observers to identify sanctions breaking vessels. Increasingly sanctions breakers will alter a vessel's features such as the colour of the deck or hull to hinder automated analysis. Key structural features may also be covered with tarpaulin.

2. Physically altering a vessel's identity.
A number of recent publications[5] provide examples in which a vessel's name and IMO number as they appear on the side of a vessel are altered. AIS transmissions will reflect the vessel's assumed identity as will all relevant documentation.

3. Altering the vessel's registered identity.
There have also been examples of where vessels have assumed a false new identity registered with the IMO as a "clean" identity for it to trade under.

[5] "Unmasked. Vessel Identity Laundering and North Korea's Maritime Sanctions Evasion" C4ADS 2021; Midterm Report of the UN DPRK Panel of Experts S/2021/777

False documents
The creation of false vessel and cargo documentation is used to deceive parties and states as to the origin of the cargo and is often seen alongside AIS manipulation. False cargo documentation will routinely misdescribe the origin or characteristics of the cargo and reference the false name and / or identity of the sanctions breaking vessel.

As part of the false identity selected for the documentation there may be a false flag. Several Flags Registries that have specific advantages for sanctions evasion are used for this. Specifically, these registries provide no easy means of communication, making it difficult to verify details. Some of the false Flag Registries may either not exist or be closed to foreign vessels. Another warning sign is vessels changing flags frequently within a short period of time, so called "flag hopping".

A further tactic observed is the use of complex business structures, including shell companies and/or multiple levels of ownership and management, to disguise the involvement of sanctioned parties in the operation of a vessel. Frequent changes to the ownership of a vessel, or the vessel's management, may also be a warning sign that something is amiss. Instances of vessels being bought, performing only one voyage from a high-risk area then being transferred to new owners just after completion of each voyage has been observed and may the involvement of parties systematically engaging in sanctioned trade operating the vessels.

Verifying false documentation is extremely challenging requiring checks and corroboration from several sources – for example do the port lists show that a vessel actually called at the port within the timeframe that it purported to load the cargo? Members may wish to check with a trusted local shipping agent in that port.

Ship to ship cargo transfer
STS operations currently present considerable risks for innocent shipowners. STS operations can be used to disguise the true origin of a cargo. A cargo may be transferred multiple times and mixed with other cargo which when combined with false or partly false documentation may make identification of the true characteristics of the cargo extremely difficult.

IG clubs have also witnessed instances in which it appears that more sophisticated sanctions breakers know when satellite imagery will be collected and take this into consideration when planning illicit STS operations.

STS operations that are used to obscure the origins of an unlawful cargo routinely take place in areas where legitimate STS operations would be expected to occur and are consistent with the false description of the cargo. For example, Iranian oil is often said to be described as of Iraqi origin with any STS operation carried out in the Persian Gulf or East Asia areas that are consistent with the trading of Iraqi oil.

STS operations should not be viewed in isolation. A legitimate operation between a vessel and a partner vessel may still present an exposure to sanctions if the partner vessel has previously engaged in an STS operation with a vessel carrying sanctioned cargo.

Consequences of sanctions breaking
Most sanctions legislation requires a failure to exercise due diligence on the part of a shipowner or other party before a breach occurs. However, in practice, States routinely act against shipowners found carrying a cargo that is deemed to be unlawful under its sanctions regime without necessarily considering the compliance procedures of the owner. States may only enforce sanctions through the criminal justice system to which the sanctions breaker is subject using designation or listing where it is domiciled elsewhere. Designation can then make it unlawful for third parties such as banks, charterers, and insurers to deal with a shipowner.

Being publicly linked with a sanction breaking activity by the press or some other public communication can be extremely damaging. The IG has seen examples of vessels declined access to ports, refusal of banking services, and removal from Flag Registries in response to unsubstantiated allegations of sanctions breaking.

Club cover is not available for unlawful trading. Cover may also be terminated where there is a risk to the Club and the provision of insurance may put the Club at risk of, or in breach of sanctions, even if the underlying trade is lawful.

Members are referred to the US Maritime Advisory, the UK OFSI Maritime Guidance and may wish to consider engaging specialist AIS sanctions software company to assist minimising the risks of an inadvertent breach of sanctions.

All clubs in the IG have issued a similarly worded circular.[6]

Yours faithfully,
GARD AS

Rolf Thore Roppestad
Chief Executive Officer

[6] The IG is grateful to Geollect Limited, www.geollect.com for their assistance in providing technical assistance for this circular.