Regulatory challenges and the new wave of technology coming to the rescue

Stringent regulations aimed at eradicating financial crime have far-reaching implications for the shipping industry, as all entities related to a vessel must be thoroughly screened for potential links to corruption before the vessel is engaged. Pinpointing potential risk, however, is not always straightforward, as **James Mirfin**, at Refinitiv reports

The impact of anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation is being felt well-beyond the banking sector and is extending into all aspects of industry, including shipping.

The implementation of regulations, including the European Fourth Money Laundering Directive (4MLD), and further changes embodied within 5MLD, along with country-specific legislation, such as Sapin II in France, require organisations to conduct thorough and rigorous due diligence before entering into any relationship with a customer or third party. More commonly referred to as know-your-customer screening (KYC), this due diligence is an ongoing requirement for many organisations.

Because risk changes through time, KYC screening needs to be refreshed and organisations must monitor third-party relationships on an ongoing basis to ensure that they are not transacting with individuals or entities linked to financial crime.

This strict regulatory landscape presents unique challenges for the shipping industry. Organisations transporting cargo by sea run the risk of unwittingly engaging a vessel that is compromised. This can result in reputational damage, financial loss, the seizure of goods and even the inclusion of individuals or companies on national and international anti-terrorist and anti-criminal watch lists.

Engaging a vessel that has previously been associated with illicit activities or currently appears on a sanctions list, such as the US Office of Foreign Assets Control (OFAC) is a significant risk, but other risks include engaging a "phantom ship" that has been hijacked, stolen, leased or bought and subsequently registered with false information about its identity, ownership, dimensions and/or characteristics.

Severe penalties

The penalties can be severe and OFAC may impose substantial criminal and civil fines. Depending on the programme, criminal penalties can range from fines of US$50,000 to $10,000,000 and even imprisonment from 10 to 30 years for wilful violations. At the same time, civil penalties can range from $250,000 or twice the amount of each underlying transaction to $1,075,000 for each violation.

Indirect risks must also be taken into account, such as investing in businesses and partnerships that have subsidiaries or associates with shipping concerns that might be involved in or associated with unethical or illicit activities. But understanding exactly who you are dealing with is not always straightforward. The true identity of a third party can be obscured by complex ownership structures making it difficult and timely to establish beneficial ownership. While there may be legitimate reasons for anonymity when it comes to ownership, there are other reasons that are just plain illegal, such as criminal activities or money laundering.

> **"As anti-money laundering legislation develops there is evidence that its impact is being felt beyond vessel ownership, reaching into financing through to marine insurance"**

The problem of beneficial ownership

The situation has been recognised by the Financial Action Task Force (FATF), the international standard setter when it comes to combatting money laundering and terrorist financing.

According to FATF, the key techniques used by criminals to obscure beneficial ownership can be categorised within three broad methods: generating complex ownership and control structures through the use of legal persons and legal arrangements; using individuals and financial instruments to obscure the relationship between the beneficial owner and the asset, including bearer shares, nominees, and professional intermediaries, and; falsifying activities through the use of false loans, false invoices, and misleading naming conventions.

As anti-money laundering legislation develops there is evidence that its impact is being felt beyond vessel ownership, reaching into financing through to marine insurance.

In April of last year, *Lloyd's List* published an article quoting Maritime and Merchant Bank as saying it was "canning up to 15 per cent of loan applications under 'know-your-customer' stipulations, with attempts to set up deals via trust companies almost certain to be rejected".

Choosing the right tools

As a company that provides regulatory technology and risk intelligence, we know how difficult it can be to implement an effective KYC programme without the right tools and data. We

© Informa UK plc 2019. No copying or sharing of this document is permitted. Enquiries: clientservices@i-law.com

Frontpage/Shutterstock.com

are seeing demand for the same tools and data we supply to the financial services sector from the shipping industry and as a result we're incorporating more shipping-related data into our services.

In March 2019, a syndicate of 15 maritime insurers based in France sought a technology solution to help support their continued compliance with legal and regulatory requirements under Sapin II and 4MLD. The Syndicat des Assureurs Maritimes de France had concerns about managing the additional compliance burden resulting from these regulations and turned to Refinitiv to help simplify their KYC processes and meet their regulatory obligations in a more reliable and cost-effective manner.

"To remain fully compliant with evolving legislation, a dynamic approach is needed and data on which decisions are based should be secured from high quality, trusted sources"

Implementing a tech-enabled approach

Although screening alone can never hope to eradicate corruption, it remains our best defence against financial crime. To fully screen for potential vessel-related risk, companies need certain key information, including the country in which a vessel is registered and the identities of all individuals and entities related to or associated with it. This information can be difficult to find, as criminals often seek to obscure vessel ownership and/or the destination of shipments.

A thorough and rigorous three-stage approach is recommended as the best strategy to mitigate maritime risk:

- As a first critical step, organisations need to ensure that they can access reliable data on all sea-going, self-propelled merchant vessels to establish identity, location and ownership information. This data should include previous vessel names and current and previous ownership structures. It should cover all IMO numbers and should be updated regularly to ensure dynamic tracking of ownership, management, name and flag changes. The goal is to screen operators, movements, ownership and names, both current and previous.
- The next step in the process will invariably focus on screening against a global risk intelligence database. An appropriate risk screening solution will help flag maritime vessels appearing on sanctions, watch and enforcement lists, including intelligence on vessels registered in, associated with, or under the flag of, an embargoed country or entity. Additionally, information on non-embargoed vessels that are directly associated with sanctioned countries, entities and individuals (even if these vessels do not appear on any sanctions or enforcement lists) should be included. Details of relevant sea ports in embargoed countries and any connections to money launderers, sanctioned entities or individuals can also be analysed with the right technology. In some instances there can also be close links to the databases of major government and transnational maritime surveillance and tracking agencies and, where relevant, records of connected registered owners and beneficial owners.
- As a final step, organisations should conduct detailed enhanced due diligence (EDD) checks on any suspicious entities flagged during the screening process.

Protect your reputation

Given the complexities of risk and the stringent nature of regulatory requirements, organisations should not underestimate the importance of taking appropriate steps to understand and pinpoint potential maritime risk. Best practice incorporates a holistic approach to identifying all vessels and related entities; and then screening these for financial crime risk before engagement. Where further investigation is warranted, EDD should be carried out. To remain fully compliant with evolving legislation, a dynamic approach is needed and the data on which decisions are based should be secured from high quality, trusted sources.

When it comes to tackling financial crime, forward thinking organisations are harnessing technology to help them cut through noise, pinpoint risk and make more informed decisions about who they do business with. ***MRI***

James Mirfin

James Mirfin, global head of financial crime and digital identity services at Refinitiv

© Informa UK plc 2019. No copying or sharing of this document is permitted. Enquiries: clientservices@i-law.com