
# Reduce your maritime anti-financial crime compliance risks

An increasingly complex, high-pressured regulatory landscape and your liability has changed.

FOR OPERATIONS DIRECTORS

INCLUDES SURVEY RESULTS

# Executive summary

# How the world of anti-financial crime compliance is changing

The anti-financial crime compliance landscape is becoming more complex and the focus has shifted toward the maritime industry. Shipping companies are increasingly facing regulatory pressures relating to anti-bribery, anti-money laundering, and sanctions compliance.

The cost of non-compliance can be severe.

## Recent regulatory changes and personal accountability

The international nature of shipping means that breaching sanctions is an ongoing risk. According to a 2020 Deloitte report, an average of 1,000 names are added to the US Specially Designated Nationals (SDN) and Blocked Persons List each year by the Office of Foreign Assets Control (OFAC).

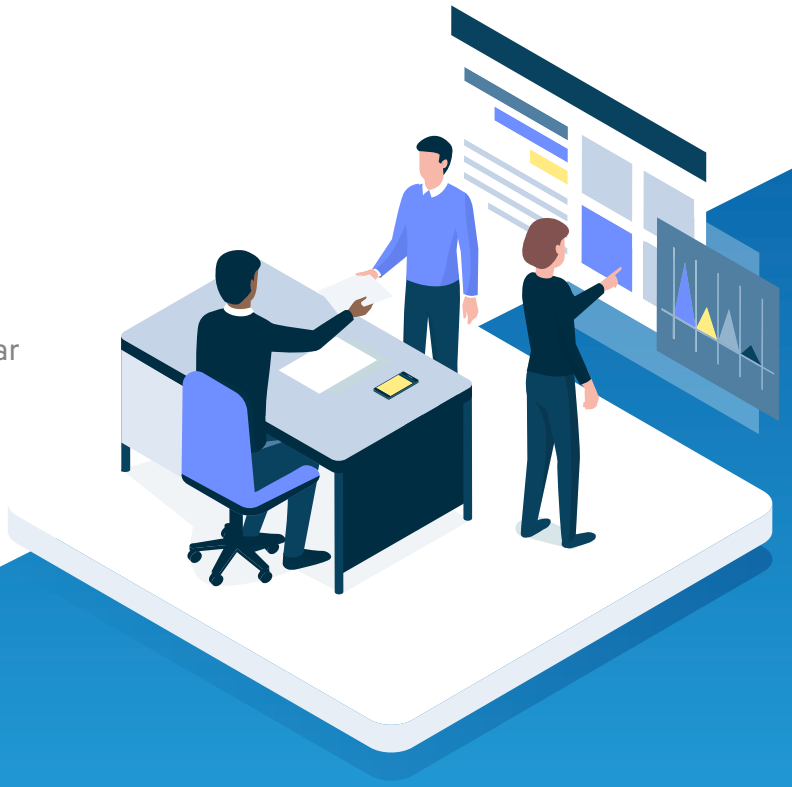
At that time, this was a high number. However, 2022 is likely to set a new record. The speed at which sanctions are now being imposed is unprecedented.

Sanctions have become a go-to political strategy, delivering financial incentives to resolve conflict rather than putting boots on the ground. The USA can quickly implement sanctions via an Executive Order (EO) signed by the US President with no requirement for action by Congress. They can be far-reaching such as the EO14071 banning all new investments in the Russian Federation, as one of President Biden's actions in response to the war in Ukraine.

As a March 2022 Alert from Holland and Knight states, "The U.S. government is well aware of and using to great effect, the reliance of international shipping trade on the U.S. financial system and the U.S. dollar, to punish Russian aggression. The U.S. dollar serves as the leading global currency. It's intricately linked to countless transactions across the maritime industry and permeates countless aspects of shipping."

The alert comes with a warning:

***"Make no mistake, the pace and scope of enforcement, including the risk of asset forfeiture and the threat of criminal or civil penalties, is quickening."***



## Procedural risks

Sanctions targeting countries such as Iran, Syria, and North Korea have been in place for a long time, but a recent OFAC prosecution outcome demonstrates the difficulty managers can have in ensuring that the right actions are taken. The situation has become more complex following the recent sanctions against Russia.

In April 2022, Toll Holdings, an international freight forwarding and logistics company headquartered in Australia agreed to pay USD6,131,855 to settle its potential civil liability for 2,958 apparent violations of multiple OFAC sanctions programs. Payments to sanctioned entities occurred over several years, between 2013 and 2019, and management of the situation was ongoing internally within Toll.

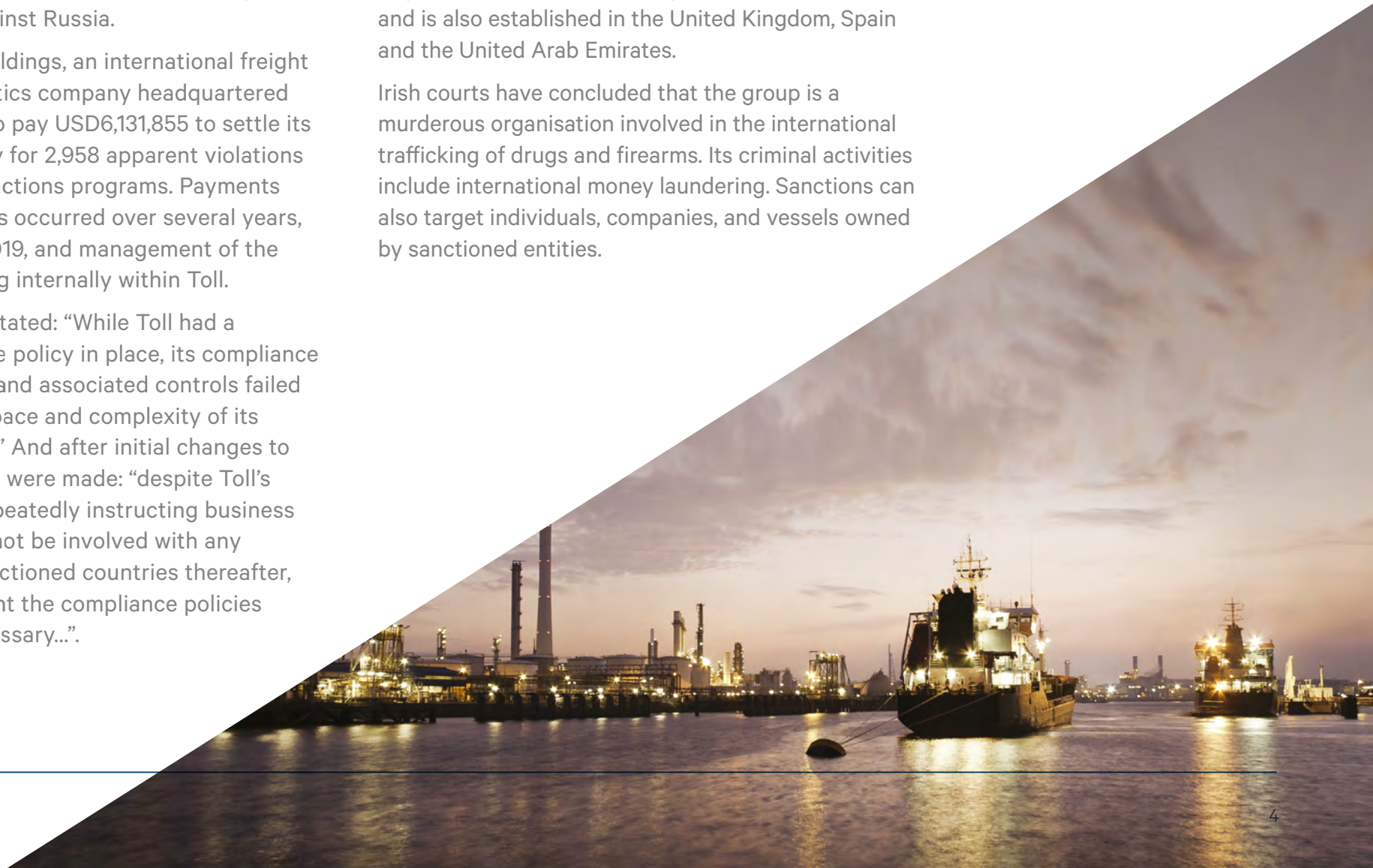
The OFAC decision stated: “While Toll had a sanctions compliance policy in place, its compliance program, personnel, and associated controls failed to keep up with the pace and complexity of its growing operations…” And after initial changes to company procedures were made: “despite Toll’s compliance office repeatedly instructing business units that Toll must not be involved with any shipments to US-sanctioned countries thereafter, Toll did not implement the compliance policies and procedures necessary…”.

## Scope of risk

While country-level sanctions are often widely discussed in the media, sanctions against organised crime groups may not be as well-known. During the Ukraine-Russia conflict, the US Department of the Treasury issued sanctions against the Kinahan Organized Crime Group. The group operates in Ireland and is also established in the United Kingdom, Spain and the United Arab Emirates.

Irish courts have concluded that the group is a murderous organisation involved in the international trafficking of drugs and firearms. Its criminal activities include international money laundering. Sanctions can also target individuals, companies, and vessels owned by sanctioned entities.

***“Sanctions can also target individuals, companies, and vessels owned by sanctioned entities.”***



## Data risks

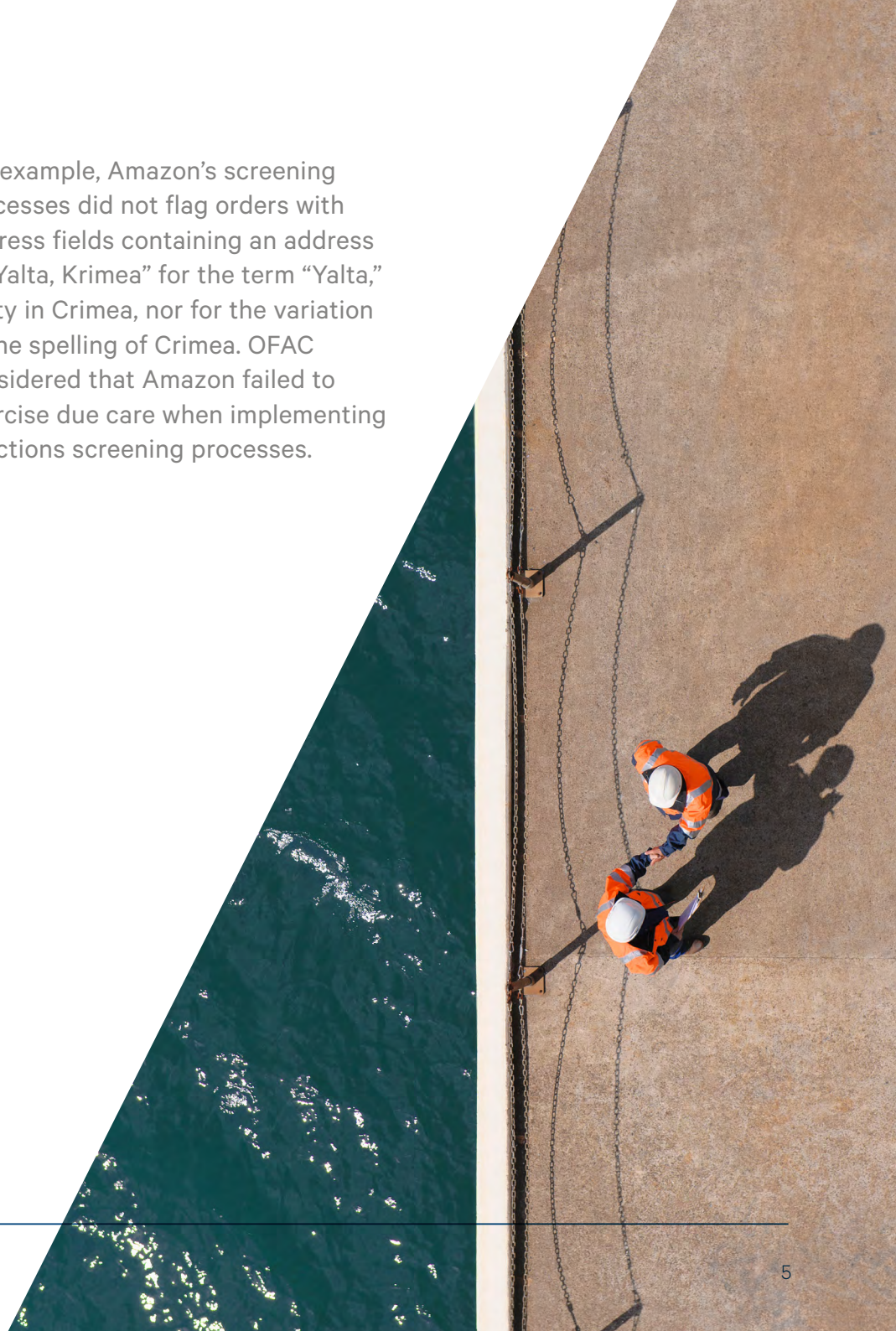
Regulators penalise companies with little to no regard of the reason or cause of a sanctions breach. For example, in 2019, OFAC announced a USD466,912 settlement with Apple, Inc. over potential civil liability for apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations, (FNKSR). The case involved dealings with SIS, d.o.o., a Slovenian software company previously identified on OFAC's List of Specially Designated Nationals and Blocked Persons as a significant foreign narcotics trafficker.

Apple later attributed this to its sanctions screening tool's failure to match the upper-case name "SIS DOO" with the lower case name "SIS d.o.o." as written on the SDN List. The term "d.o.o." is a standard corporate suffix identifying a limited liability company in Slovenia.

OFAC determined that the conduct demonstrated a reckless disregard for US sanctions requirements due to the number of apparent violations, the length of time over which they occurred and the multiple points of failure within the company's sanctions compliance program and procedures.

In a 2020 case, Amazon.com, Inc. agreed to pay a fine to settle its potential civil liability for apparent violations of multiple OFAC sanctions programs. These violations occurred primarily because Amazon's automated sanctions screening system failed to analyse all relevant transaction and customer data thoroughly.

For example, Amazon's screening processes did not flag orders with address fields containing an address in "Yalta, Krimea" for the term "Yalta," a city in Crimea, nor for the variation of the spelling of Crimea. OFAC considered that Amazon failed to exercise due care when implementing sanctions screening processes.



## OFAC's 50% Rule

The rule states that the property and interests of entities directly or indirectly owned 50% or more in the aggregate by one or more blocked persons are also considered blocked.

## UK versus EU

Both the EU and the UK have a similar rule. Brexit has added to the complexity of the international sanctions landscape. The "50% Rule" applied to sanctions against Russia is an example. According to Ropes & Gray, the UK Office of Financial Sanctions Implementation (OFSI) clarified in March 2022 that it would not automatically aggregate ownership of multiple designated persons. If each designated person's holdings are less than 50% and there is no evidence of a joint arrangement or jointly held shares, the company doesn't need to be treated as owned by designated persons and subject to sanctions.

This conflicts with the EU, which has stated that where multiple designated persons together own 50% or more of an entity, it should be treated as owned by designated persons and subject to sanctions.

The OFSI can impose monetary penalties of up to 50% of the value of the breach or up to GBP1 million, whichever is higher, for breaches of financial sanctions. It can also refer cases to law enforcement agencies. Violations of financial sanctions are considered a serious criminal offence and are punishable by up to seven years in prison.

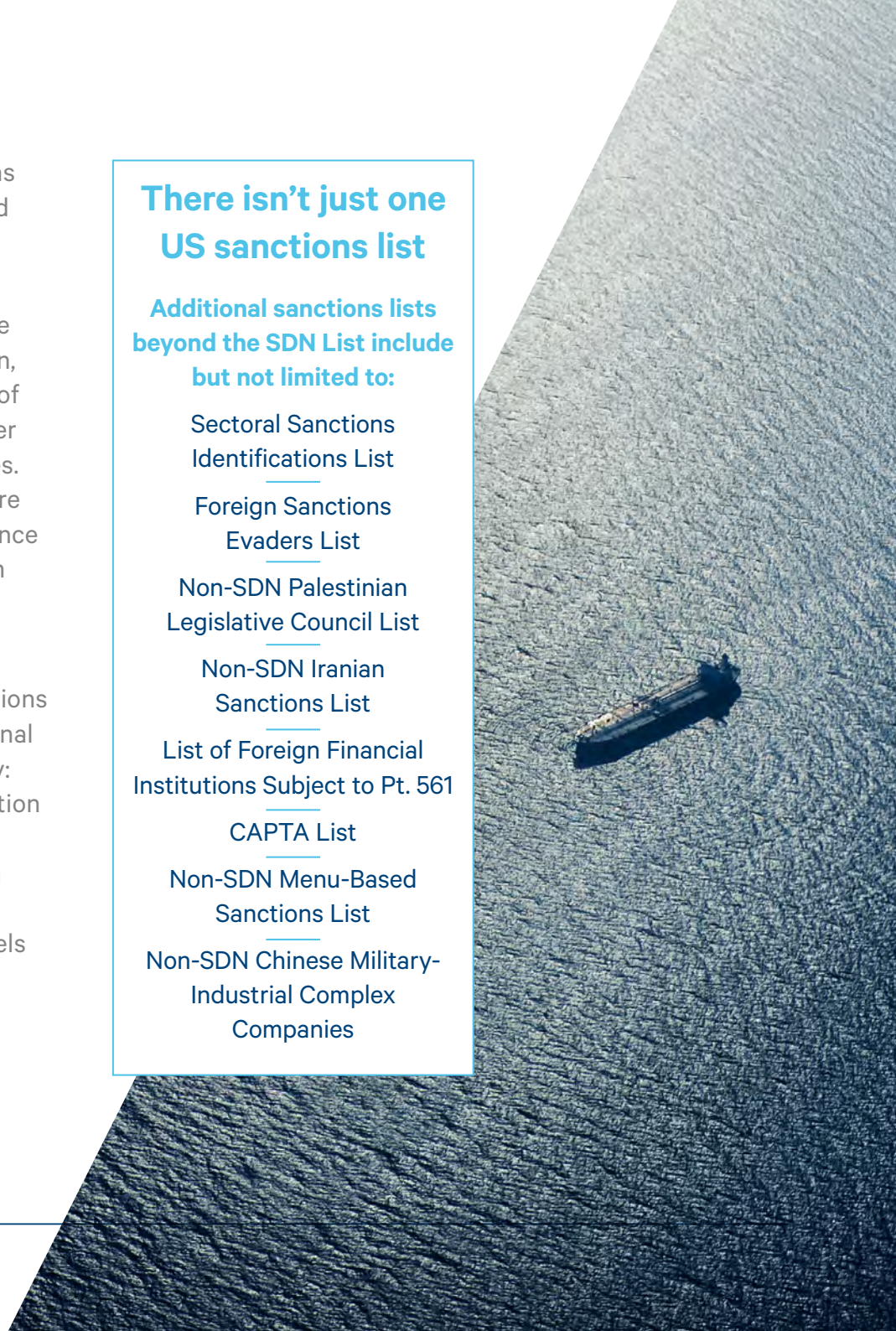
### Reputational damage

The reputational damage of violations can also be severe. The International Group of P&I Clubs noted recently: "Being publicly linked with a sanction breaking activity by the press or some other public communication can be extremely damaging. The Group 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."

## There isn't just one US sanctions list

**Additional sanctions lists beyond the SDN List include but not limited to:**

- Sectoral Sanctions Identifications List
- Foreign Sanctions Evaders List
- Non-SDN Palestinian Legislative Council List
- Non-SDN Iranian Sanctions List
- List of Foreign Financial Institutions Subject to Pt. 561
- CAPTA List
- Non-SDN Menu-Based Sanctions List
- Non-SDN Chinese Military-Industrial Complex Companies



## 6AMLD expansion – why it's crucial to know about

The European Union's 6AMLD, implemented in June 2021, has defined 22 offences which constitute money laundering and introduced significant changes in liability which are of particular importance to Operations Directors.

Whereas previous versions of the Directive only punished those who profited directly from money laundering, the 6AMLD expands the regulatory scope by penalising anyone who assists money launderers.

This means that managers, directors, and CEOs are now responsible for having the systems in place to prevent and detect crimes within their organisations. Additionally, criminal liability is extended by including not only individuals but also entities such as companies or partnerships.

Maximum prison sentences have been increased, and penalties include fines and bans on conducting business in the future. Natural persons will now face up to four years imprisonment for money laundering offences. Penalties for legal entities include the closure of the establishment, which has been used for committing the offence.

Member states are increasing their cooperation in investigating and prosecuting cross-border money laundering. Other regulators, such as the Monetary Authority of Singapore, Australia's Department of Foreign Affairs & Trade, and Japan's Ministry of Foreign Affairs, have similar regulations in compliance with the requirements of the global watchdog, Financial Action Task Force (FATF) requirements.

## Greater vigilance

The global banking sector has become more compliance-focused after some big names in the industry were prosecuted. Deutsche Bank is an example. New York's Department of Financial Services said the bank helped convicted sex offender Jeffrey Epstein transfer millions of dollars between 2013 to 2018, including more than USD7 million to resolve legal issues and more than USD2.6 million in payments to women, covering tuition, rent, and other payments.

In a statement, the bank said: "We acknowledge our error of onboarding Epstein in 2013 and the weaknesses in our processes and have learned from our mistakes and shortcomings. Our reputation is our most valuable asset, and we deeply regret our association with Epstein."

The take-away for shipping companies is that banks are intensifying their adverse media screening when onboarding customers, especially in view of the 6AMLD's expansion of predicate offences. Banks are also enhancing their transaction monitoring systems.

***"The European Union's Anti Money Laundering Directive introduced significant changes in liability which are of particular importance to Operations Directors"***

## ‘Dear CEO’ Letter

In September 2021, the UK Financial Conduct Authority (FCA) and the Bank of England’s Prudential Regulation Authority (PRA) jointly warned the country’s top banks that they must improve oversight of their trade finance businesses after a spate of scandals that caused hundreds of millions in losses and allowed criminals to abuse the financial system. One case involved supply chain finance company Greensill Capital which collapsed earlier that year and is now facing criminal allegations related to its relationships with several parties.

The “Dear CEO” letter ordered recipients to conduct a full financial crime risk assessment of their processes to detect potential violations among their clients related to money laundering, terrorist financing, sanctions evasion, and fraud. The letter cites challenges in global trade: “There are inherent risks within trade finance activity, given that it can be complex, global in nature and the large volumes of trade flows utilising multiple currencies.”

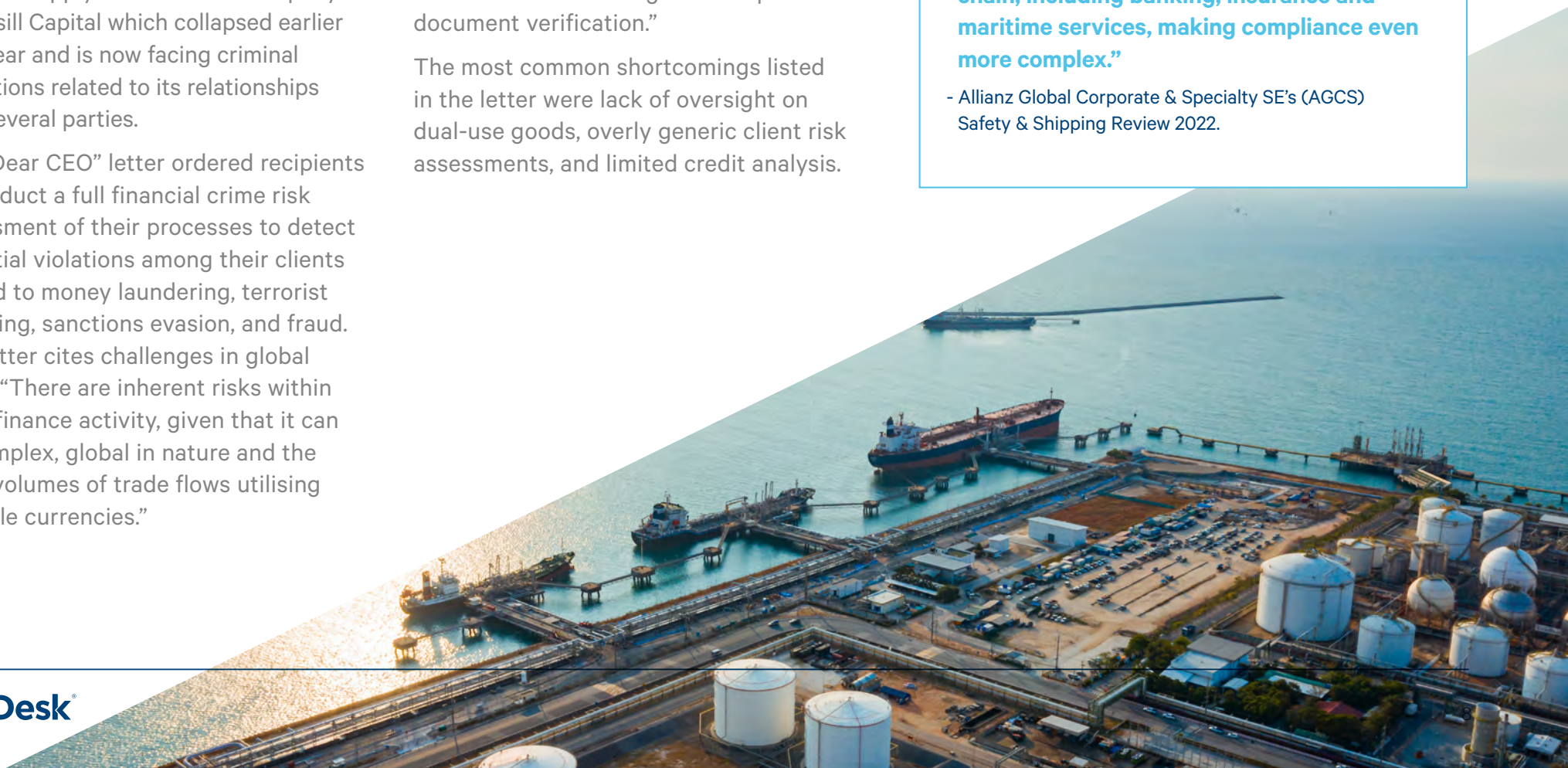
The letter explicitly references maritime compliance: “We have found that firms have either failed to assess these risks, are unable to evidence the checks they have undertaken, or in some cases discounted them inappropriately. Failure to assess or understand these risks can lead to insufficient due diligence, such as additional pricing checks or using tools such as vessel tracking and independent document verification.”

The most common shortcomings listed in the letter were lack of oversight on dual-use goods, overly generic client risk assessments, and limited credit analysis.

**“The evolving range of sanctions against Russian interests presents a sizeable challenge. Violating sanctions can result in severe enforcement action, yet compliance can be a considerable burden.**

**Establishing the ultimate owner of a vessel, cargo, or counterparty can be difficult. Sanctions apply to the transport supply chain, including banking, insurance and maritime services, making compliance even more complex.”**

- Allianz Global Corporate & Specialty SE’s (AGCS) Safety & Shipping Review 2022.



## The Marlboro Canal

For a long time, shipping companies and seafarers have been subjected to corrupt demands, such as unlawful requests for payments to allow ships to enter and depart ports or disproportionate penalties for minor errors. This can lead to interruptions in operations, delaying vessels and creating a risk to navigation and seafarer safety.

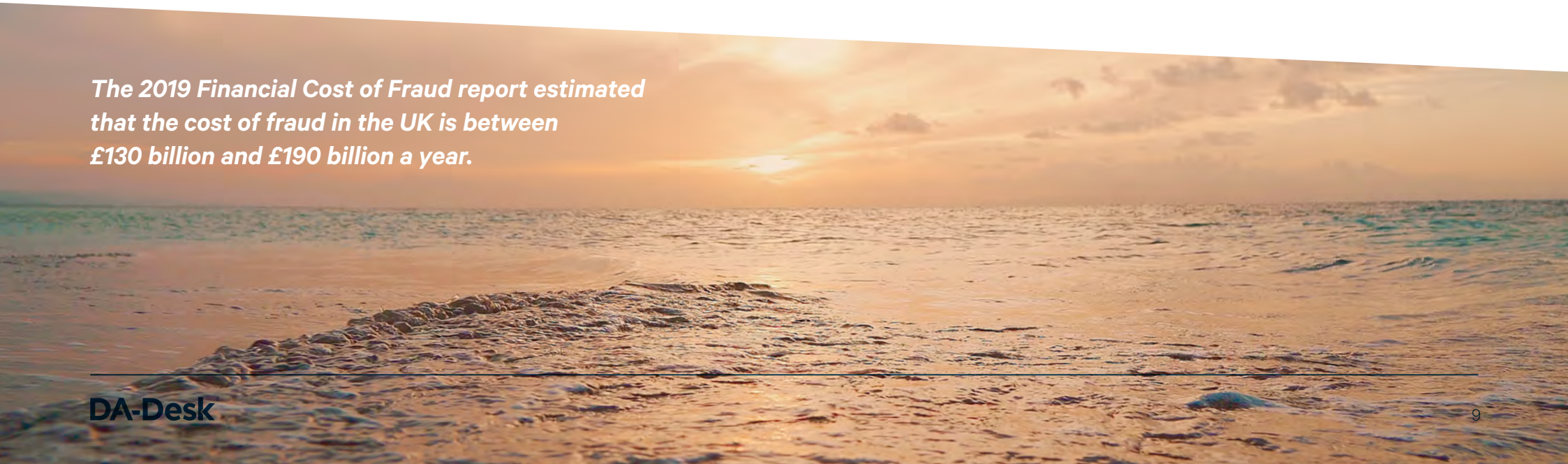
The Suez Canal, sometimes nicknamed the "Marlboro Canal," is an infamous example. Some Suez Canal Authority (SCA) staff have been accused of collecting boxes of cigarettes as facilitation payments. However, in March 2022, the SCA sent a letter to the International Chamber of Shipping stating that all shipping companies transiting the canal should refuse to hand out facilitation payments. The letter was also sent to local shipping agencies. The Authority uses digital transactions to avoid bribery and investigates reported cases of corruption.

## Scammers

Shipping companies, like all companies, and their employees can be victims of many other forms of corruption. The 2019 Financial Cost of Fraud report estimated that the cost of fraud in the UK is between GBP130 billion and GBP190 billion a year. The Office for National Statistics says that people are more likely to fall victim to fraud or cyber offences than any other crime.

Fraudulent correspondence can be challenging to spot. A maritime scam was brought to the attention of Action Fraud, the UK's national reporting centre for fraud and cybercrime, in 2022. A seller of second-hand shipping containers, S Jones Containers, recently raised the issue of an increasing number of people falling victim when trying to buy a shipping container through platforms such as Gumtree, Amazon, and eBay. The sellers impersonated S Jones Containers, using company branding, staff photos, and dummy email addresses, and often sent invoices with seemingly legitimate details.

Their advice: if the price seems too good to be true, it is.



## Trouble within

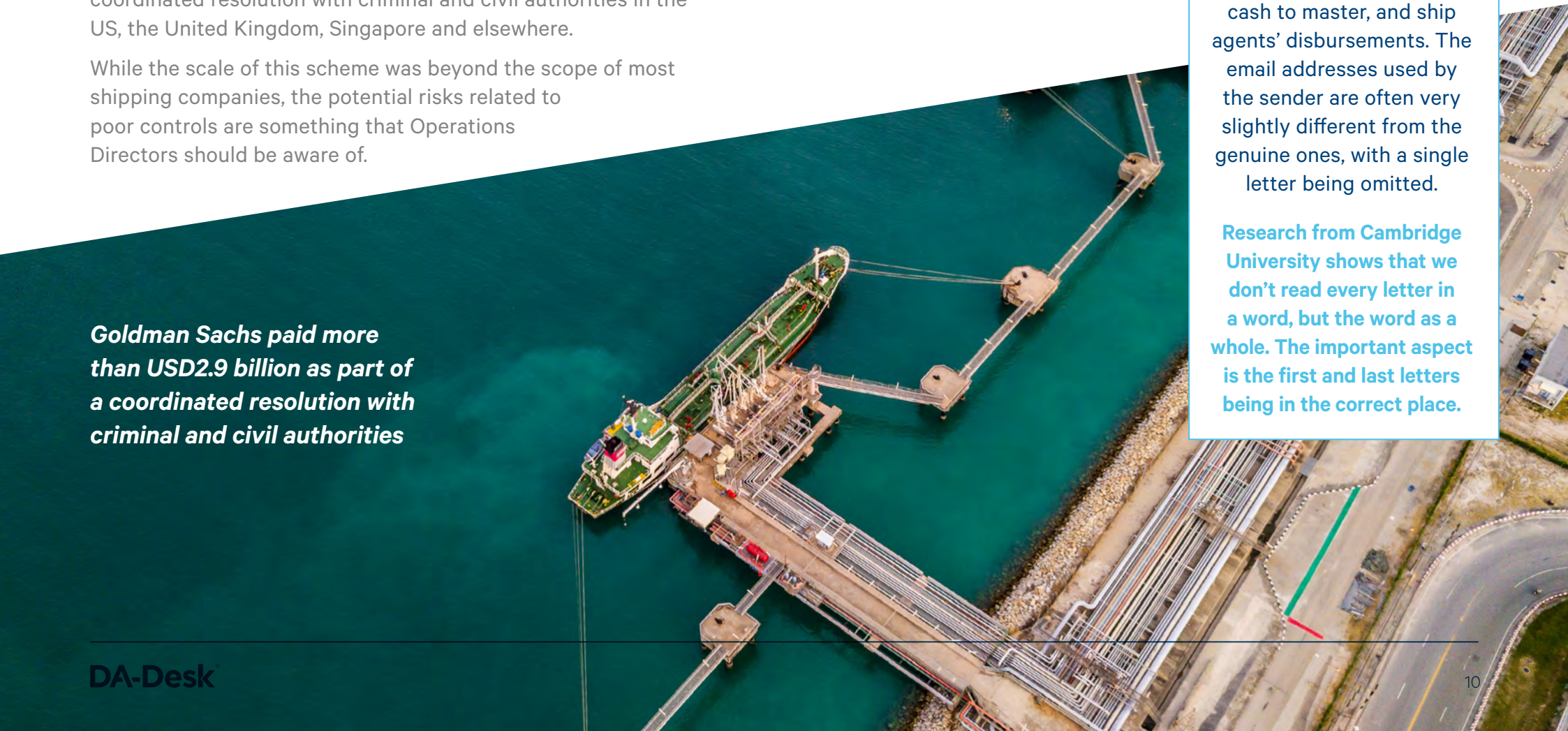
Sometimes trouble comes from within companies. In April 2022, the US Department of Justice announced the conviction of a former Managing Director of The Goldman Sachs Group Inc. for conspiring to commit bribery, circumventing internal accounting controls, and committing money laundering in connection with a multibillion- dollar scheme involving Malaysia's state-owned investment and development fund. Goldman Sachs paid more than USD2.9 billion as part of a coordinated resolution with criminal and civil authorities in the US, the United Kingdom, Singapore and elsewhere.

While the scale of this scheme was beyond the scope of most shipping companies, the potential risks related to poor controls are something that Operations Directors should be aware of.

## Risk management

The above examples of increasing high-profile legal cases in light of new regulations highlight the dynamic environment in which shipping companies operate. It is essential to have the appropriate governance, risk management, and compliance measures in place. Read on to see what this entails.

***Goldman Sachs paid more than USD2.9 billion as part of a coordinated resolution with criminal and civil authorities***



## BE ALERT

Cyber fraud can occur when a party due to make a payment receives a fraudulent message altering the recipients' bank details. Examples include diverting freight payments, hire, cash to master, and ship agents' disbursements. The email addresses used by the sender are often very slightly different from the genuine ones, with a single letter being omitted.

**Research from Cambridge University shows that we don't read every letter in a word, but the word as a whole. The important aspect is the first and last letters being in the correct place.**

SURVEY RESULTS

# How Operations Directors view the challenges

Operations Directors and senior management from across the maritime industry gave their views on anti-financial crime compliance. Most ranked AFC compliance as a top concern, and the key concerns raised were scams changing remittance details, maintaining confidentiality, sanctions compliance and fraud prevention.

## 8/10 Respondents

Find it hard to keep up with maritime AFC changes

**SANCTIONS**

**PHISHING**

**KYC**

**LAUNDERING**

## Top 4

Anti-financial crime compliance concerns


Find it difficult to do all the required counterparty, KYC and other AFC checks as part of processing DA's

**76%** Feel focusing on AFC compliance checks on DAs is now more important

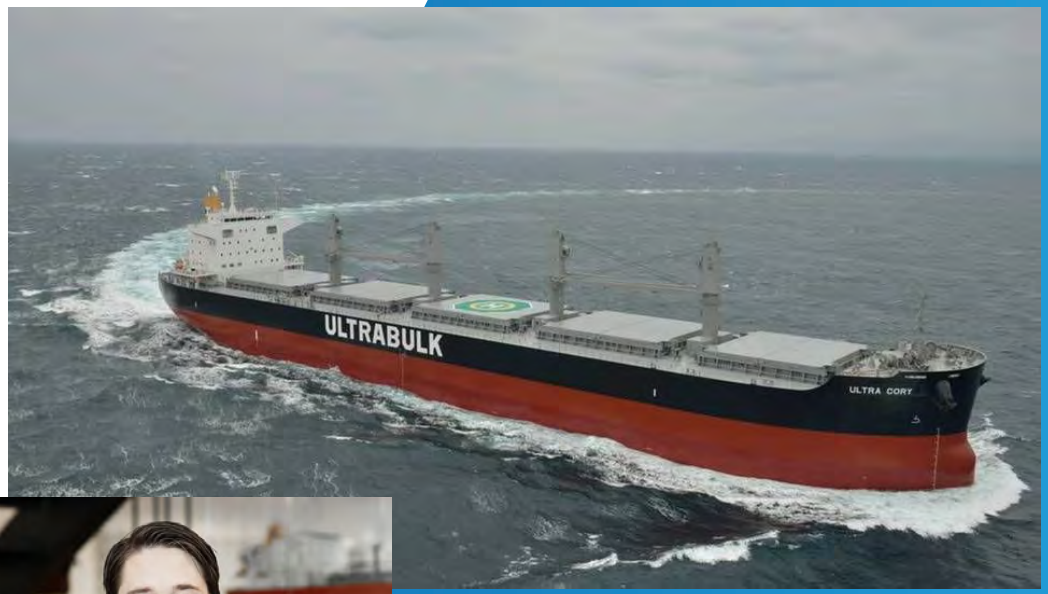
CASE STUDY:

# Having the right resources for compliance checks

"Anti-financial crime compliance is definitely on our agenda," says Oskar Fabricius, CFO, Ultrabulk, a leading global dry bulk operator. "It's something that is difficult to control as one company, for the many counterparties that we deal with in the ports. Last year our revenue was close to USD2 billion, but we only have 140 people."

He says everything around compliance is taking an increasing amount of time. "It's something that we are thinking more and more about – knowing our counterparties, knowing what they are doing and how that affects us. In terms of manpower, it's a concern, and it's not something that we can take on ourselves."

The company relies on the scale and scope of DA-Desk, especially when the choice of an agent at a given port is often dictated by the charterer, and Ultrabulk may not have prior knowledge of the company. "It's key that there's a company in between that has the resources and enough customers to be able to mitigate the risks."




Ultrabulk™

DA-Desk®

CASE STUDY:

# Outsourcing compliance efforts to reduce risk

"Financial risk is complex to manage," says Dorte Thuesen Christensen, VP for Operations and Claims at Hafnia, a leading product tanker owner and operator. "If you have a breach in the system, in your processes or procedures, it becomes a very open loop where laws can be breached, and money lost. We partner with a specialised company, with a strong compliance profile, enabling us to manage our risk position at a more proactive level."

Hafnia has clearly identified the risks of violating sanctions, and the potential for fraud. "Emails come through the system that attempt to convince us to modify our bank account details and remit funds. That's a gigantic risk, and we are very much aware of that. It's on me, my operations, our finance and IT departments and our legal team to be prepared and this is something we constantly work against across our organization."

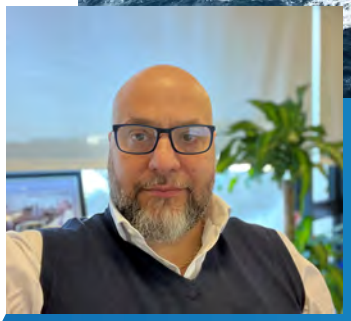
With DA-Desk, Dorte rarely needs to consider DA-specific AFC compliance checks. "It's not an aspect that is front of mind, because it's being managed. We haven't experienced any problems arising from either internal or external audits."

The benefits of using DA-Desk extend beyond risk mitigation. "I find myself a more attractive employer because compliance checks are an undesirable task. By delegating this, I increase the engagement of my team. They can focus on what is adding value, and on the more motivating tasks."

CASE STUDY:

# The increasing AFC risks and how DA-Desk makes life easier

"Anti-financial crime compliance is something that we think about every day, every minute, every second," says Giuseppe Oliveri, Fleet Manager at d'Amico Group, a leader in the dry cargo and product tanker sectors. "We were discussing this with DA-Desk last week, how compliance on their side works compared to ours. Because no matter whether you do the checks on your side, we need to do them on ours. And if we can add them together, it's better for all of us. Everything needs to be continuously checked. Today an agent can be cleared; tomorrow, the agent is not cleared anymore. The risks are always increasing, and DA-Desk makes my life easier."

d'Amico

Compliance is a team effort for Giuseppe. "If you make dumb mistakes and work with the wrong company, the business could be closed down completely. It's not my responsibility, not an individual responsibility, it is a group responsibility. That doesn't mean that the weight is taken off my shoulders. The responsibility belongs with each one of us."

## Moving forward

These industry insights led DA-Desk to raise awareness of the issues and lead the discussion on how anti-financial crime risks can be addressed. We are ready to help the industry move forward confidently.

# Reduce your AFC compliance risks in shipping

The maritime industry faces some tough anti-financial crime compliance challenges, including the need to keep up-to-date with potentially thousands of agents around the world, having multiple voyage-associated parties across various jurisdictions and facing the opaque ownership of ships and assets.

Additionally, anti-financial crime regulations can vary significantly across countries and can change almost daily. The current fluid compliance environment is expected to last, so inaction isn't an option for Operations Directors who want to sleep well at night. We will set out here some generally accepted guidelines which can assist with managing compliance:

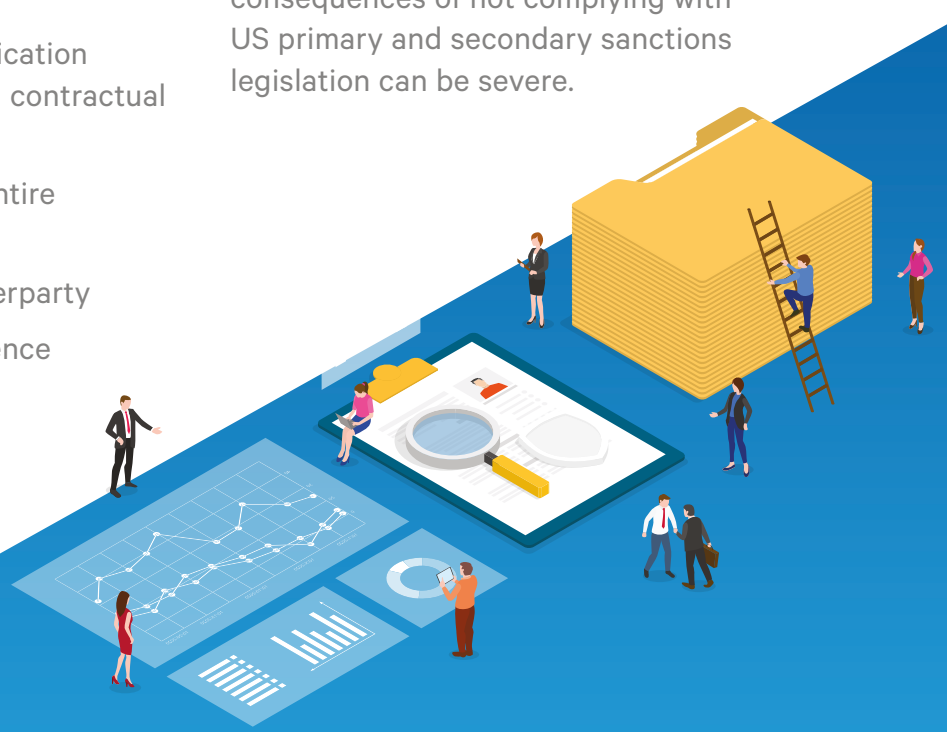
## Follow the funds

The US Government issued a 35-page Guidance in May 2020 that provides specific guidelines on due diligence and other compliance-related activities.

It lays out a non-exhaustive list of best practices companies can adopt to prevent sanctions violations, providing clear guidance to insurers, ship owners, operators, brokers, crewing companies, and ship captains. It recommends that companies appropriately assess their sanctions risk, implement compliance controls to address any gaps in their compliance programs, and adopt the following best practices:

- institutionalise sanctions compliance programs
- establish ship automatic identification system (AIS) best practices and contractual requirements
- monitor ships throughout the entire transaction lifecycle
- know your customer and counterparty
- exercise supply chain due diligence
- incorporate specific compliance clauses into contracts

The International Group of P&I Clubs notes that the guidance places heavy emphasis on the need to perform proper know your customer (KYC) and know your customer's customer (KYCC) procedures. The way in which many commodities are traded renders this a complex area, and the consequences of not complying with US primary and secondary sanctions legislation can be severe.



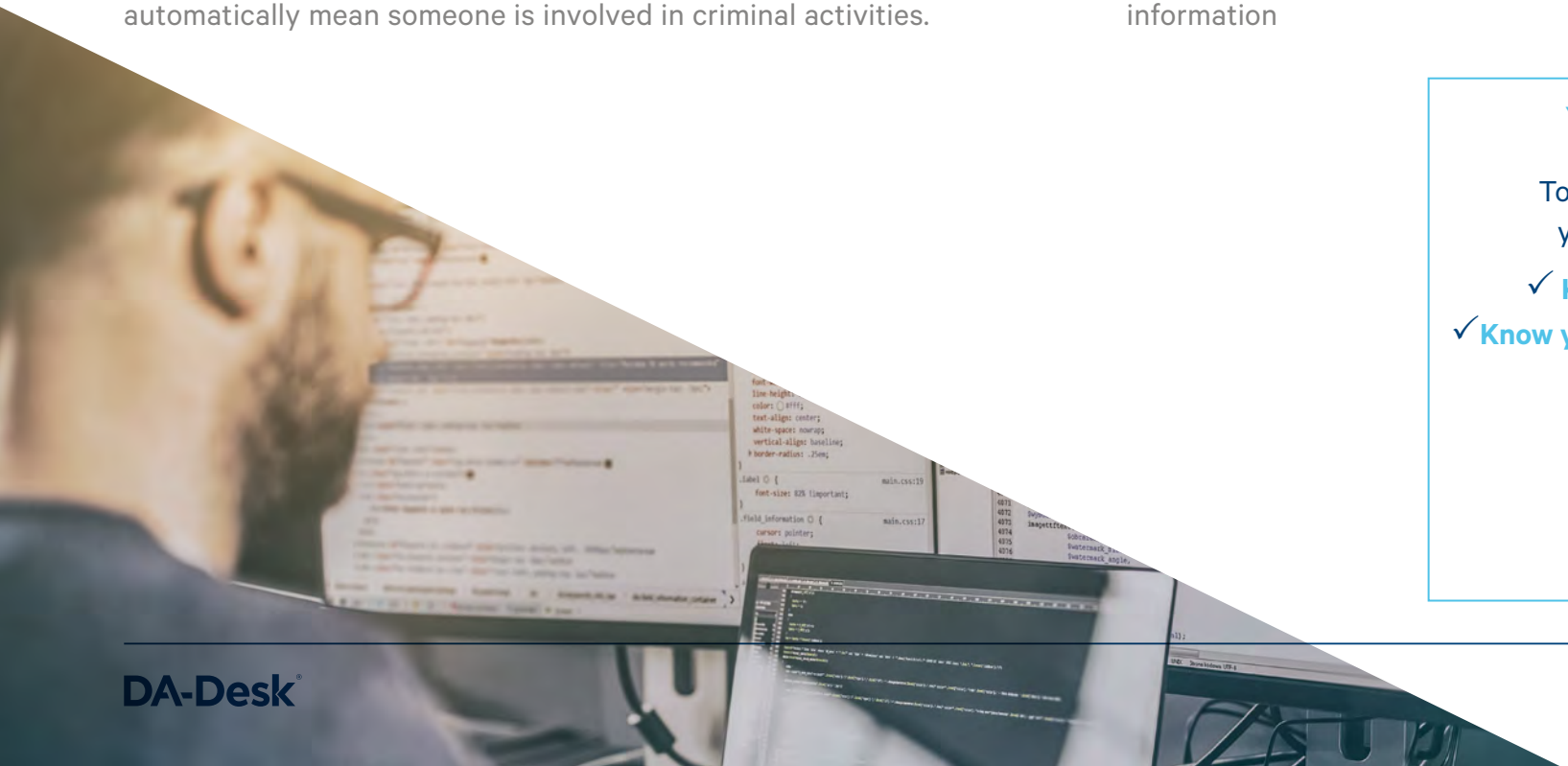
## Know your counterparty (KYC)

KYC procedures include identifying politically exposed persons (PEPs) and other high-risk individuals when engaging the services offered by shipping agents. Even engaging a well-established agent in a seemingly low-risk port involves some level of risk and the legal and financial circumstances of an agent and other service providers can change at any time.

A PEP is an individual who holds a prominent public position or role in a government body or international organisation. Immediate family members and/or close associates of these individuals are also considered PEPs. Examples of PEPs include government ministers and senior executives, judges, military leaders, or senior executives or board members of a government-owned organisation. Because they hold positions of influence, they can be a target for corruption, bribery, or terrorism financing activities. However, being a PEP doesn't automatically mean someone is involved in criminal activities.

Shipping companies can take inspiration from the US Financial Crimes Enforcement Network (FinCEN) Customer Due Diligence (CDD) Rule issued in May 2018, designed to improve financial transparency and prevent criminals and terrorists from misusing companies to disguise their illicit activities and money laundering.
The CDD Rule has four core requirements:

- identify and verify the identity of customers
- identify and verify the identity of the beneficial owners of companies opening accounts
- understand the nature and purpose of customer relationships to develop customer risk profiles
- conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, maintain and update customer information



### You need to know

To secure your reputation and your business, you need to:

- ✓ **Know your customers (KYC)**
- ✓ **Know your customers' customer (KYCC)**
- ✓ **Know your crew**
- ✓ **Know your agents**
- ✓ **Know your suppliers**
- ✓ **Know your vessels**
- ✓ **Know your partners**

## Monitoring risk

Operations Directors should ensure that continuous monitoring programs are in place to keep up to date on the latest sanctions and other regulations. In June 2020, the US Department of Justice (DOJ) published an updated version of its guidance on the Evaluation of Corporate Compliance Programs.

It reflects the DOJ's continued expectation that companies must evolve and enhance their compliance programs and makes clear that companies should continuously check that it's working by:

- monitoring, evaluating, and revising business risks on an ongoing basis
- ensuring the compliance function has the necessary resources
- adapting the compliance program to address the companies' needs and risk appetite
- empowering the compliance function through access to actionable data for timely and effective monitoring and/or testing of policies, controls, and transactions

The Financial Action Task Force (FATF), the global group that sets international anti-money laundering and counter-terrorism financing standards, regularly publishes updates, such as those published in March 2022, which inform about jurisdictions that may pose a risk to the international financial system:

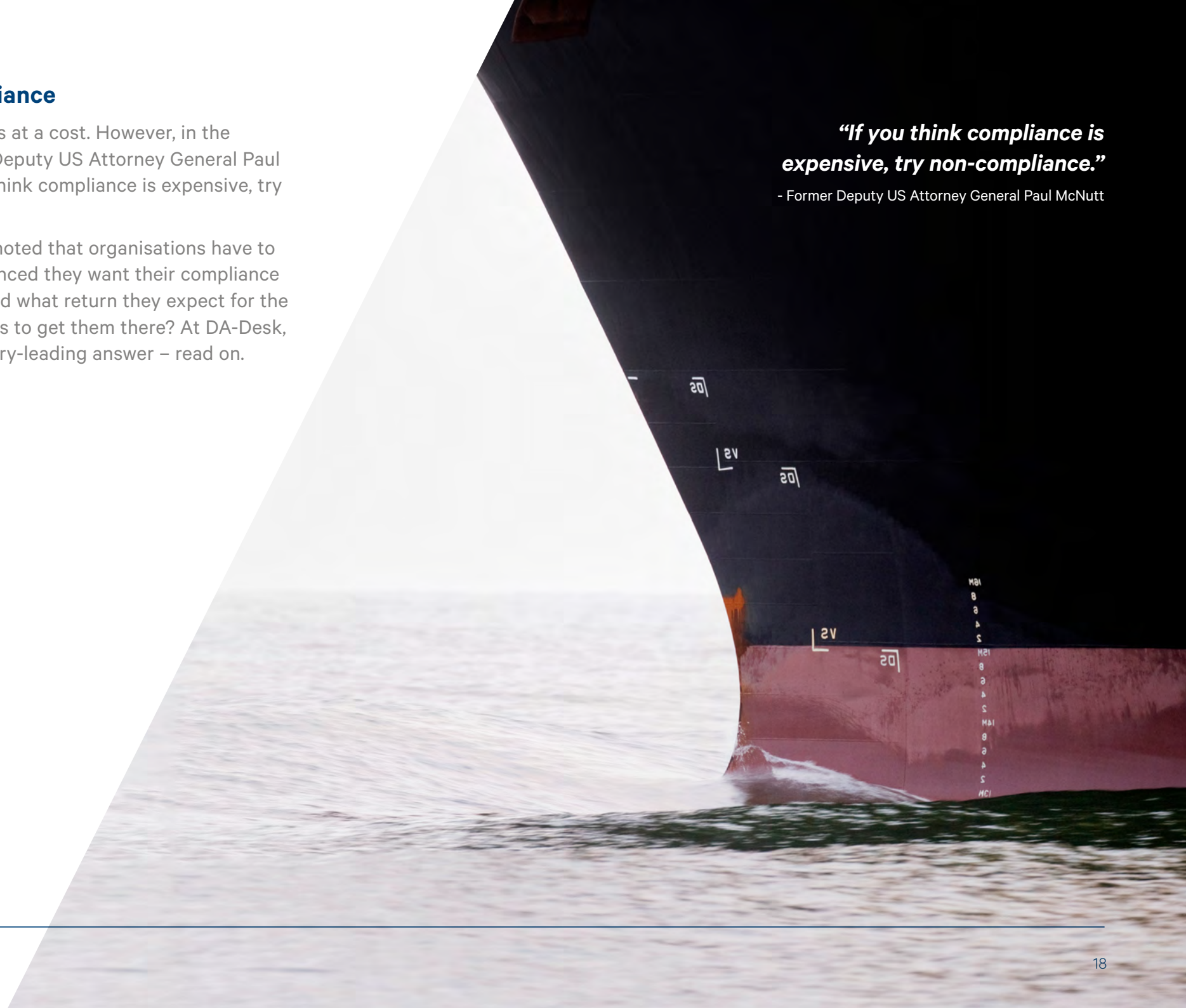
- High-Risk Jurisdictions subject to a Call for Action – March 2022 – notes that the 21 February 2020 call for action in relation to the Democratic People's Republic of Korea and Iran remains in effect
- Jurisdictions under Increased Monitoring – March 2022 – lists jurisdictions with strategic deficiencies in their anti-money laundering and counter-terrorism financing regimes and are actively working with the FATF to address them

The IMO has developments underway that shipping companies should keep updated on. The IMO commenced the development of guidance on anti-corruption in 2017 when the Maritime Anti-Corruption Network (MACN) initiated a cross-industry working group together with the International Chamber of Shipping. In June 2021, the 45th session of the IMO's Facilitation Committee (FAL 45) agreed to re-establish an IMO Correspondence group to continue developing IMO guidance to address bribery and corruption in the maritime sector.

## Cost of compliance

Compliance comes at a cost. However, in the words of Former Deputy US Attorney General Paul McNutty: “If you think compliance is expensive, try non- compliance.”

Deloitte recently noted that organisations have to choose: how advanced they want their compliance functions to be and what return they expect for the investment it takes to get them there? At DA-Desk, we have an industry-leading answer – read on.



***“If you think compliance is expensive, try non-compliance.”***

- Former Deputy US Attorney General Paul McNutt

# DA-Desk helps reduce your anti-financial crime compliance risk


DA-Desk enables you to automate and streamline due diligence, mitigate the risk of fraud and provide evidence of regulatory compliance.

Every port call is screened, including every appointment, every proforma disbursement account (PDA), and every final disbursement account (FDA).

DA-Desk's built-in compliance service delivers trade and economic sanctions compliance, Know Your Counterparty (KYC) checks, bank account verification, information security compliance, payment approval and transaction monitoring, anti-financial crime (AFC) screening, Sarbanes-Oxley Act compliance, and Disbursement Account validation checks.

## Trade & economic sanctions compliance

Using data from multiple providers such as Dow Jones and Accuity, DA-Desk carries out screening and checks against:

- global sanctions lists including OFAC, OFSI, EU, US, UN, and other country-specific lists
- specially designated nationals (SDN) and non-SDN lists
- other official lists such as INTERPOL, state-owned entities, tax defaulters, amongst others

## Know Your Counterparty (KYC) checks

Obtain KYC data and perform risk-based due diligence on your agents, vendors, and suppliers.

Cleanse and enhance the KYC data, including:

- establishing if the name is a trading name or a legal registered name
- perform verification of the address and contact details
- obtain and screen ultimate beneficial owner (UBO) information; and obtain source of funds information

## Bank account verification

- Continuous screening of beneficiary names and banks with IBAN/SWIFT validation
- Perform enhanced due diligence if you receive a request to make a payment to a jurisdiction different from that of the relevant counterparty

## Information security

We have prevented over a hundred fraudulent and phishing attempts in the past few years, saving our customers and agents over USD5 million that would otherwise have been lost to fraud.

## Payment approval and transaction monitoring

- Perform continuous and ongoing daily screening of all the relevant entities (including vessels) in our database
- Check published tariffs and benchmark data to check expenses in the DA
- Pre-payment and post-payment checking to help ensure payments are processed successfully – if not, we get involved to resolve it
- Running screening checks again on the bank and the beneficiaries of the payment seconds before payments are released to our banking provider

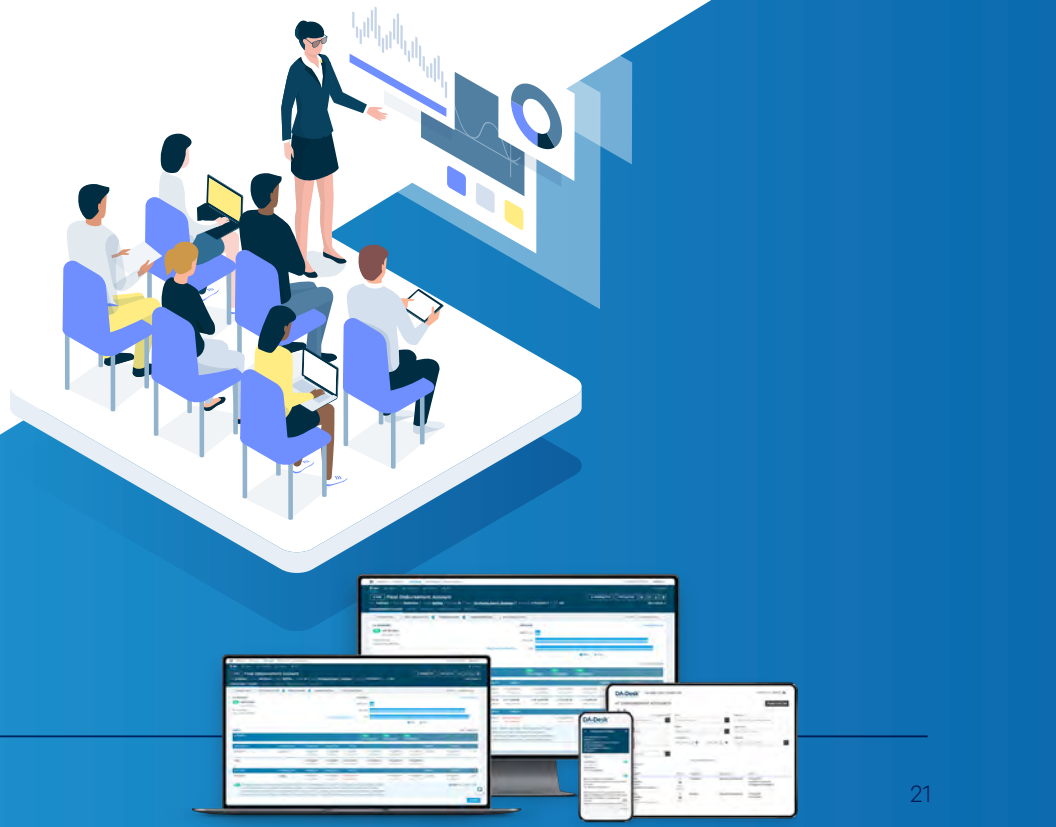
## Anti-financial crime (AFC) screening

- Screen all DAs and invoices and will not process an expense without supporting documentation
- Perform fraudulent attempt checks, sanctions, politically exposed persons (PEPs), and adverse media screening

## Sarbanes-Oxley (SOX) Act compliance

We are audited (Deloitte's annual ISAE 3402 Type II audit), to complement and support your SOX compliance requirements:

- DA-Desk controls are appropriately designed, tested, and implemented, complementing customers' audit requirements
- Full record trail, books, and records compliance. The DA-Desk platform allows for the uploading, collation, review, and retention of all supporting port call-related documentation



## Invoice and DA validation

DA-Desk checks DAs and invoices for irregularities and inconsistencies in the value of those invoices – we do this by combining our specialists and automation. DA-Desk's proprietary system, which does this, is named DA Validation Engine (DAVE).

Issues that arise are resolved directly by the DA-Desk team, providing you with two benefits:

- direct cost savings (please click here for more information); and
- an added check on the legitimacy of invoices for fraud prevention, AML, and ABC.

## DA-Desk assurance

Our IT systems, internal & external audits, controls, and certifications give you confidence in DA-Desk as your compliance partner.

Our processes and controls are certified and compliant with:

- ISO 9001 Quality Management System
- ISO 27001 Information Security Management System
- ISO 14001 Health, Safety & Environment Management System
- ISO 45001 Occupational Health & Safety Management System
- EU & UK GDPR – General Data Protection Regulation
- ISAE 3402 Type 2 Report – Annual Service Auditor's Report