WorldECR

ISSUE 77. MARCH 2019
www.WorldECR.com

Survey says Brexit will hit investment and operations in controlled goods

With the UK's scheduled date for its departure from the European Union only one month away as at time of writing, a *WorldECR* survey suggests that the prospect of a no-deal Brexit is already filling some in the trade compliance world with a degree of trepidation.

WorldECR polled the views of 50 of its UK/European readers, asking them for their views on a range of Brexit-related issues.

Amongst our findings are:

- Of those who responded, all predict some degree of disruption to supply chains involving dual-use or military goods.
- Companies in the controlled goods sector have already begun contingency planning for a no-deal Brexit.

The *WorldECR* survey has identified an expectation that export compliance will become more burdensome after Brexit.

- Over half of respondents (57%) agree that in the event of a no-deal Brexit it will be necessary for companies in the controlled goods supply chain to move some operations out of the United Kingdom.
- One-third of respondents believe jobs in the controlled goods sector will be affected.
- All respondents believe that export compliance will become more burdensome for UK companies. 75% believe the same for EU companies.
- 57% of respondents believe that investment into the controlled goods supply chain will be adversely affected.

Any positives? Yes, but not glaring: More respondents believe that the UK government has given clear advice about export controls in the event of a no-deal Brexit than those who think that it hasn't. Let's hope that those hard-toiling civil servants can keep up the good work 'in the unlikely event that the UK leaves the European Union without a deal.'

All respondents believe that export compliance will become more burdensome for UK companies.

UK 'on wrong side of the law' re Saudi arms exports

The UK government's policy of licensing arms sales to the Kingdom of Saudi Arabia is 'narrowly on the wrong side of the law', according to a House of Lords Select Committee on International Relations.

In its report, 'Yemen: giving peace a chance', the Committee members say that they 'recognise that there are legitimate reasons for UK arms exports overseas. Export licensing decisions for the sale of arms always require fine judgements, balancing legitimate security concerns against human rights implications, and each situation must be assessed individually. The Government asserts that, in its licensing of arms sales to Saudi Arabia, it is narrowly on the right side of international humanitarian law.'

But, the Committee members note, in their opinion, 'Although conclusive evidence is not yet available, we assess that [the Government] is narrowly on the wrong side: given the volume and type of arms being exported to the Saudi-led coalition, we believe they are highly likely to be the cause of significant civilian casualties in Yemen, risking the contravention of international humanitarian law.'

Amongst its conclusions, the Committee said that the UK 'should immediately condemn any further violations of international humanitarian law by the Saudi-led coalition, including the blocking of food and medical supplies, and be prepared to suspend some key export licences to members of the coalition.'

It also said that the UK government should 'signal that failure by Saudi Arabia, the United Arab Emirates or Iran to back the Stockholm Agreement in deeds as well as words would have negative consequences for our relations with these countries.' Under the Stockholm Agreement, parties agreed a ceasefire in the city and port of Hodeidah in order to allow supplies to reach those that need them.

The charity Médecins Sans Frontières estimates that some three million people have been displaced in Yemen since 2015, and 20 million people are in need of humanitarian assistance.

The report, 'Yemen: giving peace a chance', is at:

https://publications.parliament.uk/pa/ld201719/ldselect/ldintrel/290/29003.htm#_idTextAnchor024

News and alerts

Iran settlements show dangers of weak supply chain compliance measures

Two recent settlements between the Office of Foreign Assets Control ('OFAC') of the US Department of the Treasury and US companies show the continuing compliance dangers of doing business in the proximity of Iran.

The experiences of Zag IP and Kollmorgen serve as a strong reminder of the need for full and ongoing due diligence around Iran-related trade.

Transhipment risk reminder

On 21 February, OFAC released details of a settlement with Connecticut company Zag IP, in the sum of $500,000.

According to OFAC, on five separate occasions in 2014 and 2015, Zag had purchased around 260,000 metric tons of Iranian-origin clinker 'from a company located in the United Arab Emirates, with knowledge that the cement clinker was sourced from Iran, and then resold and transported it to a company in Tanzania.'

The value of the transactions was around $14.5m.

The settlement explains that ZAG had signed a supply contract with a company based in Tanzania and agreed to supply about 400,000 metric tons of cement clinker manufactured by a company based in India.

The settlement notes: 'Under the terms of the contract, ZAG was required to supply the Purchaser with a minimum of three shipments of cement clinker in 2014 and a minimum of five shipments in 2015 (about 50,000 metric tons per each shipment).

'On or about June 26, 2014, the Supplier sent an email to ZAG's Managing Director of the Asia Pacific, Middle East, and East Africa Regions ("ZAG Managing Director") that, due to a technical problem at its production plant, it would not have sufficient cement clinker to load onto ZAG's vessel on or about July 5, 2014. ZAG attempted to reschedule the date of its first shipment to the Purchaser but was unable to do so after the Purchaser objected to any delays and threatened to cancel the entire contract.'

The ZAG Managing Director then found an alternative supplier who could source Iranian-origin cement clinker, and, 'Relying on the Alternative Supplier's misrepresentation that the cement clinker was not subject to U.S. economic sanctions on Iran, ZAG purchased the alternative cement clinker from the Alternative Supplier despite its knowledge that the goods were produced by an Iranian manufacturer and shipped from a port in Iran.'

Amongst the aggravating factors, OFAC notes: '

1. Although ZAG did exercise limited due diligence, it acted with reckless disregard for sanctions requirements by failing to substantively address the U.S. sanctions prohibitions in place with respect to Iran despite contemporaneous risk indicators;
2. ZAG's senior management was aware that ZAG was purchasing and reselling goods of Iranian origin at the time of the conduct at issue;
3. the transactions giving rise to the apparent violations conferred significant economic benefits to Iran;
4. ZAG is a commercially sophisticated company operating globally with experience and expertise in international transactions; and
5. ZAG did not have an effective OFAC compliance program in place at the time of the transactions commensurate with its level of risk.'

OFAC commented: 'It is essential that companies engaging in international transactions consider and respond to sanctions-related warning signs, such as information that goods originating from, being loaded or unloaded at ports located in, or trans-shipping through, countries or regions subject to comprehensive U.S. economic and trade sanctions.'

'Paltry' settlement disguises sanctions 'shot across the bows'

Earlier in February, Virginia-based Kollmorgen settled with OFAC to the tune of $13,381 so as to put to bed liability for six apparent violations of the Iranian Transactions and Sanctions Regulations ('ITSR') on behalf of a Turkish affiliate, Elsim.

According to the settlement document, Kollmorgen acquired control of Elsim in 2013, hiring external consultants and lawyers to perform sanctions due diligence on the company. Finding that Elsim did have business with Iran, Kollmorgen took 'extensive' steps to ensure that from the date of its acquisition it would be fully compliant with US law.

Nonetheless, according to OFAC, 'In spite of Kollmorgen's extensive efforts to ensure Elsim complied with the ITSR, for two years after acquisition,

'[Kollmorgen] marks the first time ever that OFAC has sanctioned an individual as a foreign sanctions evader in conjunction with the resolution of an enforcement case.'

Elsim willfully, and with full knowledge of the applicable prohibitions, dispatched employees to Iran to fulfill service agreements and engaged in other transactions related to Iran. Elsim management threatened to

continues over

fire employees if they refused to travel to Iran. Upon returning from the service trips in Iran, Elsim employees were directed by Elsim management to falsify corporate records by listing the travel as vacation rather than business related.'

After discovering the 'apparent violations', Kollmorgen fired the managers responsible and put in new procedures. OFAC said that had there not been mitigating factors (including extensive remedial conduct), the base penalty would have been $750,000.

In addition to the action, OFAC is sanctioning Evren Kayakiran, the Elsim manager it regards as 'primarily responsible for the conduct that led to the Apparent Violations' under Executive Order 13608, Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria.

In a briefing on the Kollmorgen case, John E. Smith, former Director of OFAC and now co-head of Morrison & Foerster's national security practice, noted that while the 'paltry $13,381 settlement reflected the small dollar value of the materials and services provided and the fact that Kollmorgen had implemented a wide range of pre- and post-acquisition sanctions compliance measures before and after it acquired control of Elsim in 2013', in the unprecedented portion of the case, 'OFAC also sanctioned individually the manager primarily responsible for the Turkish affiliate's violations and added him to its Foreign Sanctions Evaders List. This marks the first time ever that OFAC has sanctioned an individual as a foreign sanctions evader in conjunction with the resolution of an enforcement case.'

Smith said that the case should serve 'as a reminder to US parent corporations that, in the context of the Iran sanctions, it is they who will pay for the sins of their overseas subsidiaries [and a] a warning shot across the bow to officials abroad that they may face individual liability if they incur the wrath of OFAC.'

Links and notes

For the Zag settlement, see:
https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190221_zag.pdf

The Kollmorgen settlement is at:
https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20190207_kollmorgen.pdf

US senators reintroduce bill on Russia

President Trump's 'willful paralysis' in the face of Kremlin aggression has reached 'a boiling point in Congress'.

So said Senator Bob Menendez in words accompanying the introduction of proposed legislation which would 'increase economic, political, and diplomatic pressure on the Russian Federation in response to Russia's interference in democratic processes abroad, malign influence in Syria, and aggression against Ukraine, including in the Kerch Strait.

'The legislation establishes a comprehensive policy response to better position the US government to address Kremlin aggression by creating new policy offices on cyber defences and sanctions coordination. The bill stands up for NATO and prevents the President from pulling the US out of the Alliance without a Senate vote. It also increases sanctions pressure on Moscow for its interference in democratic processes abroad and continued aggression against Ukraine.'

If put into law, the Defending American Security from Kremlin Aggression Act ('DASKA') of 2019, would, amongst other things impose: '

Senator Bob Menendez is behind the bill.

- Sanctions on Russian banks that support Russian efforts to undermine democratic institutions in other countries
- Sanctions on investment in Russian LNG projects outside of Russia
- Sanctions on Russia's cyber sector
- Sanctions on Russian sovereign debt
- Sanctions on political figures, oligarchs, and family members and other persons that facilitate illicit and corrupt activities, directly or indirectly, on behalf of Vladimir Putin.'

https://www.menendez.senate.gov/news-and-events/press/senators-introduce-bipartisan-legislation-to-hold-russia-accountable

UK implements EU blocking statute

Legislation is now in force in the United Kingdom which criminalises activity in contravention of the EU blocking statute – e.g., compliance with US sanctions where not compatible with EU law.

In June 2018, following the announcement of the US withdrawal from the Joint Comprehensive Plan of Action ('JCPOA' or 'Iran nuclear deal'), the EU amended (to include the reversal of the US position on Iran) its original blocking statute of 1996, which was drafted to 'counteract the effects of the extra-territorial application of laws, including regulations and other legislative instruments adopted by third countries, and of actions based thereon or resulting therefrom, where such application affects the interests of natural and legal persons in the Union engaging in international trade and/or the movement of capital and related commercial activities between the Union and third countries.'

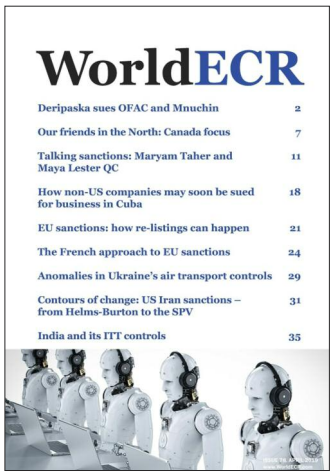
The UK implementing law is the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) (Amendment) Order 2018.

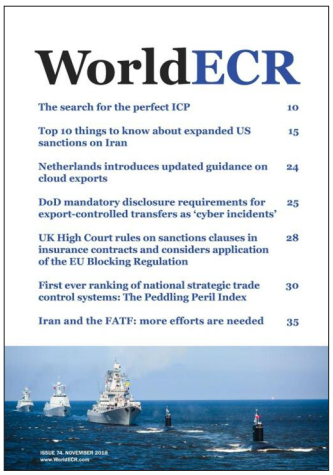
The UK legislation is at:
http://www.legislation.gov.uk/uksi/2018/1357/pdfs/uksi_20181357_en.pdf

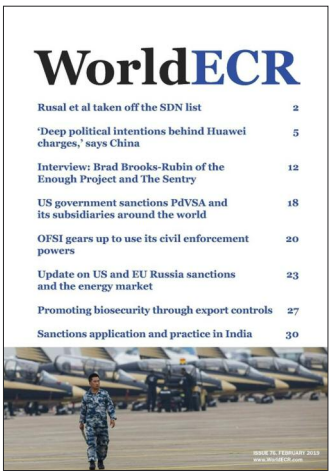
SUBSCRIBE TO WORLDECR

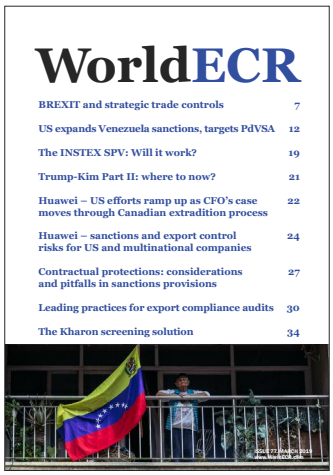
Launched in 2011, WorldECR (World Export Controls Review) is today established as the leading journal covering developments in - and offering insight into - the increasingly important and fast moving areas of **export controls** and **economic sanctions**.

Published ten times a year in pdf format, WorldECR keeps its readers in touch with what is happening in export controls and sanctions around the world - like export compliance departments, it is a business enabler.









Our subscribers include manufacturers of defence, dual-use and technology items; global logistics and supply chain management organizations; governments; U.S. national laboratories; academic institutions; multilateral export control regimes... and the law firms who advise them.

There are two subscription options:

1) Single-site subscription - this provides the pdf journal to an unlimited number of readers in a single office/site of the subscribing organisation for a year (10 issues) - costs £329

2) Multi-site subscription - this provides the pdf journal to an unlimited number of readers in more than one office of the subscribing organisation for a year (10 issues) - costs £449

Both options can be upgraded to include access to the Archive of all back issues (goes back to 2011) for an extra £100 per year.

To subscribe or to find out more about subscriptions to WorldECR, please visit **www.worldecr.com/subscribe** or contact publisher, Mark Cusick at **mark.cusick@worldecr.com**

We look forward to welcoming you as a subscriber.

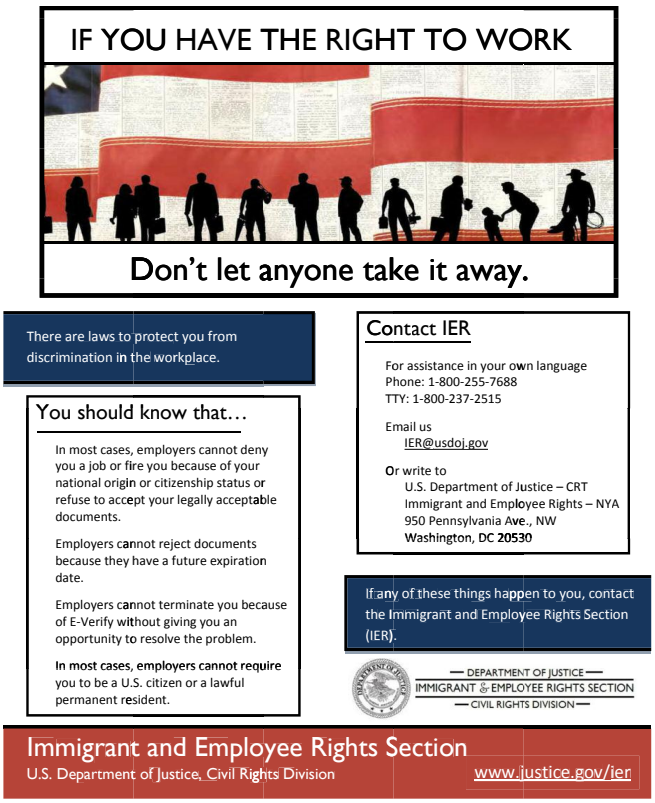
‘You have the right to work’ – even on ITAR projects – says the US DoJ

In imposing a blanket ban on some categories of person applying for ITAR-related roles, Honda Aircraft Company breached US Department of Justice Immigrant and Employee Rights (‘IER’) Section discrimination rules, the US Department of Justice (‘DoJ’) has said, announcing a ($44,600) settlement with the company.

In the settlement document, the DoJ says that ‘by publishing job announcements from at least August 2015 through December 2016, specifying that only applicants who are lawful permanent residents and/or U.S. citizens would be considered for employment in the advertised positions, without legal justification for those citizenship status restrictions and implementing the published restrictions in hiring for the positions,’ the company engaged in hiring discrimination.

The settlement is the culmination of an independent investigation by the IER, and notes that ‘neither the ITAR nor the EAR require employers to restrict hiring to U.S. citizens or lawful permanent residents, but instead permit covered entities to hire, without obtaining a license or other approval, all “U.S. Persons,” including, *inter alia*, lawful permanent residents, citizens or nationals of the United States, refugees and asylees.’

Amongst the terms of the settlement are that it ‘…shall not discriminate, including by directing any third party to discriminate pursuant to a contract or other means, on the basis of citizenship, immigration status or national origin in violation of 8 U.S.C. § 1324b. Respondent also shall not intimidate, threaten, coerce, or retaliate against any person for his or her participation in the IER Investigation or the exercise of any right or privilege secured by 8 U.S.C. § 1324b,’ and, ‘If not already posted, Respondent shall post an English and Spanish version of the IER's “If You Have The Right to Work” poster (“IER Poster”), in color and measuring no smaller than 8.5" x 11", an image of which is available at https://www.justice.gov/crt/page/file/926651/download, in all places where notices to employees and job applicants are normally posted.’



The IER's “If You Have The Right to Work” poster.

https://www.justice.gov/opa/press-release/file/1126521/download

UK lawmakers in pocket of Russian politicians – Browder

The Russian government and individuals are paying members of the UK political establishment to prevent sanctions designations being made under the Magnitsky Amendment – and succeeding in their efforts. So said Bill Browder, architect and proponent of the Magnitsky Act in the United States and beyond, addressing a UK parliamentary inquiry into the use of sanctions.

In his evidence, Browder said that following the enactment of the Financial Sanctions Act (which includes the Magnitsky Amendment) in the summer of 2018, he expected swift implementation of the law, noting that in all the other countries in which similar acts have been passed – including the United States, Canada, Lithuania, Latvia and Estonia – sizeable numbers of designations have been made of Russians and others, for human rights abuses; whilst in the UK by comparison, ‘that number is zero’.

Browder refuted the official reason given, he says, by the UK government for its failure to take steps under the act – that it isn’t possible to do anything until after the UK’s departure from the EU – arguing that not only did he have it on good academic and legal authority that the UK is not so prevented, but also that Lithuania, Latvia and Estonia are also EU Member States which have made Magnitsky designations. ‘I’m sad to say,’ he said, ‘that people connected to the political process are trying to influence the government to not make life difficult [for those that might be included on such a list].’ Such people, he said, included members of the House of Lords, who had received money from individuals, and former government officials and advisers who had received money to [minimise] sanctions consequences.

Browder said he advocated an absolute ban on UK lawmakers lobbying on behalf of foreign governments and supported the enactment of a law comparable to the US Foreign Agents Registration Act.

‘[The UK] is the go-to country for dictators and kleptocrats – because they know that they won’t be harassed…It requires a complete change in government culture in how to deal with them,’ he said.

Iran's foreign minister resigns post

Iran's foreign minister Javad Zarif, who took a key role in the Iranian delegation negotiating the Joint Comprehensive Plan of Action ('JCPOA') with the United States and other members of the P5+1, resigned from the post on 26 February. It is not yet clear whether his resignation has been accepted by President Hassan Rouhani.

Iran's Fars News describes Zarif as 'the most favorite man in [Rouhani's] cabinet.'

The Iranian news agency IRNA confirmed the veracity of Zarif's announcement, made on the social media platform Instagram. It said: 'Congratulating the auspicious birth anniversary of Hazrat Fatemeh (AS), Day of Mother in Iran, Zarif appreciated the Iranian nation for their nobleness. He also begged pardon for his incapability of continuing his services and all probable deficiencies during his tenure.'

Iran's foreign minister Javad Zarif, who has resigned his post

IRNA has also reported Zarif (who has been urged by MPs not to resign) as describing the country's foreign policy as having been 'poisoned' by political infighting and factionalism.

Observers have noted that Iran's moderate faction – of which Rouhani and Zarif are the most prominent members – are stuck between the proverbial rock and hard place: the JCPOA is crippled by the Trump administration's withdrawal, despite the efforts (including the creation of INSTEX – see article in this issue) made by other members of the negotiating coalition to keep it alive, and has thus failed to provide Iran with any kind of dividend (indeed, the value of the rial has plummeted since 'Implementation Day').

The JCPOA's failure has bolstered hard-liners in the Iranian administration who had always distrusted the US position – in turn, providing the US administration justification for increasing economic pressure on Iran.

In an article explaining the Trump administration's strategy in Iran, US Secretary of State Mike Pompeo wrote in October 2018 that the goal 'of these aggressive sanctions is to force the Iranian regime to make a choice: whether to cease or persist in the policies that triggered the measures in the first place. Iran's decision to continue its destructive activity has already had grave economic consequences, which have been exacerbated by officials' gross mismanagement in pursuit of their own self-interests. Extensive meddling in the economy by the IRGC [Islamic Revolutionary Guard Corps], under the guise of privatization, makes doing business in Iran a losing proposition, and foreign investors never know whether they are facilitating commerce or terrorism.'

US State Department officials will, no doubt, be asking whether Zarif's resignation, if accepted, brings them closer to the diplomatic conciliation Pompeo seeks.

Australia concerned to control new technologies

Australia's Defence Export Control Organisation ('DECO') has given its backing to recommendations made by an independent parliamentary review of the Defence Trade Control Act ('DTC Act').

Amongst the gaps identified in the DTC Act are 'the lack of control over the transfer of technology not captured by the DTC Act's existing provisions but which, if transferred to foreign entities with interests contrary to Australia's, could prejudice Australia's security, defence and international relations.'

The review also identified 'the inadequate control of emerging and sensitive military and dual-use technology' as something that needs to be addressed.

In its response to the review, the government has said that 'the Defence Exports Controls Branch (DEC) will establish a working group, led by an independent person, to develop options to address the identified gaps in the Defence Trade Controls Act 2012 (DTC Act). The working group will consist of representatives from Defence and other relevant government agencies and university, industry and SME representatives to develop practical, risk-based legislative proposals to amend the DTC Act to enhance the government's ability to prevent the transfer of defence and dual-use technology to entities that may use it in a manner contrary to Australian interests or who are acting on behalf of a foreign power.'

http://www.defence.gov.au/publications/reviews/tradecontrols/Docs/Initial_Government_Response.pdf

Going places

Kevin Cuddy, formerly Senior Manager International Trade at GE Global Operations, has taken a role with IBM's Export Regulation Office in Washington DC. Cuddy told *WorldECR* that he is looking forward to working on 'cutting-edge compliance issues, from artificial intelligence to cloud computing to encryption controls.'

In London, export controls and sanctions lawyer **Roger Matthews** has left Dechert for Dentons where he joins as a partner. Matthews has experience in government as well as in private practice, having worked at HM Treasury and the Bank of England. Dentons' CEO for Europe and the Middle East said that the firm is 'delighted that someone of Roger's calibre has decided to join us at a time when many firms in the UK are looking to build up their capabilities in this area.'

Taking back control?

What does BREXIT actually mean for strategic trade controls? *WorldECR* investigates.

Brexit is coming. And despite government reassurances over the past two years that the UK exiting the EU without a deal is 'unlikely', the odds are growing shorter on a hard Brexit on 29 March. *WorldECR* asked trade lawyers, industry associations and in-house counsel what issues are on the path to resolution, and what remains uncertain for exporters at this critical juncture.

More certainty on dual-use exports...

The UK Export Control Joint Unit ('ECJU')'s new open general export licence ('OGEL') authorising the export of dual-use goods to the EU in the case of a no-deal Brexit, issued in early February, was warmly welcomed by the tech industry.

'The new OGEL is looking good; we just have some minor concerns around the edges,' says Craig Melson, programme manager in charge of export controls, environment and compliance at industry body TechUK. 'The issue of this technical notice shows that the government has listened to industry concerns.'

The types of technologies controlled by the UK and the EU should remain broadly similar, as the UK is a member of the international export control regimes that underlie the EU's export control framework, such as the Wassenaar Arrangement. But this does not rule out the creation of separate EU or UK autonomous lists of controlled items in future.

The new dual-use OGEL complements a proposal in the European Commission ('EC')'s December contingency plan, which set out a 'bare bones' plan to maintain trade flows in the case of a no-deal Brexit. This proposal advocated an amendment to the EC Dual-Use Regulation (Council Regulation (EC) No 428/2009) to include the UK in the list of 'safe' destinations covered by Union General Export Authorisation ('UGEA') No. EU001, which currently covers countries such as the US, Japan, Norway and Canada. The regulation is currently in draft form. 'It is not clear at the moment whether the timeline will allow the UK to be added by 29 March,' says Sophie Delhoulle, director of legal services and trade compliance for the EMEA region at Accenture.

...but logistical uncertainty remains

The same level of comfort has not been provided on the physical processes of customs and exports, which are still a cause of major anxiety; an acute one for industries relying on 'just in time' delivery, such as parts for the automotive or aerospace industries, or fresh produce, in the case of agri-food businesses. It is these UK-based companies that have been particularly vocal on the need to clear the fog of Brexit: Airbus, Jaguar Land Rover and the major supermarkets, including Asda and Marks & Spencer. The prospect of licensing requirements between the EU and the UK also affects businesses further afield, including US tech companies with global distribution networks.

'US tech companies which produce controlled items such as encryption products currently might rely on an export permit issued by one EU Member State authorising them to distribute goods from anywhere in the EU to other countries outside the EU,' says Melissa Duffy, an international trade partner at Dechert. 'After Brexit these will no longer be valid for the UK.'

A particular concern for these businesses is the logistics of servicing or repair, rather than sales, as items may be sent from a regional distribution centre to a depot in the UK that fulfils this function. 'These companies are having evaluate their supply chains that run to and through Europe to consider new licensing requirements and take pro-active measures to deal with the prospect of a no-deal Brexit,' says Duffy.

Melson echoes these sentiments: 'There is concern over inward

News feature: Brexit

processing – not necessarily exporting for sale, but the logistics of repair, or reconfiguration,' he says. 'We don't yet have a full understanding of the problems.'

What is HMRC doing to prepare for Brexit?

HMRC, the UK government's revenue and customs department, has contacted over 145,000 UK companies which will have to register as exporters for the first time to outline the procedures for applying for both an economic operator registration identification ('EORI') number and the new transitional simplified procedures ('TSP'), which will allow goods (with the exception of controlled goods) to be transported to the UK without making a full customs declaration. The TSP will also allow for import duties to be postponed.

So far, so sensible. March will be a challenging month for HMRC, as unless there is a cancellation or extension of Article 50, it faces a double whammy: Brexit, in its current unfathomable form, and the final phasing in of its new Customs Declaration Service ('CDS') to all exporters. CDS replaces the 25-year-old Customs Handling of Import and Export Freight system ('CHIEF') – which processes declarations for goods exported between the UK and non-EU countries – with 'a modern and flexible system that can handle anticipated future import and export growth', according to the UK government.

The CDS system is being phased in in stages and some of its export functions are still being tested. The lack of feedback on its effectiveness is frustrating for exporters:

'The pre-filling out works well for military items, because they have more obvious end uses,' says Melson. 'Dual-use items are trickier.'

At the moment those involved in the testing have to sign non-disclosure agreements, but this may be revised.

After years of austerity, HMRC has finite resources. Prior to the referendum result, it was anticipated that the CDS would handle around 100 million trade declarations per year. Following Brexit, the volume of customs declarations is estimated to rise to over 350 million declarations. In its analysis of HMRC's 2017-18 performance, the Public Accounts Committee raised concerns over possible delays to the CDS and questioned HMRC's capacity to handle 'postponed accounting' in the event of no-deal Brexit. 'HM Revenue & Customs is under pressure and in some areas the cracks are showing,' said committee chair Meg Hillier MP.

It is unclear whether the mutual recognition benefits of authorised economic operator ('AEO') status will be maintained after Brexit.

This doubt is echoed by trade: 'There are concerns over the capacity workload for customs,' says Brinley Salzmann, director of overseas exports for ADS, the trade organisation for companies in the UK aerospace, defence, security and space sectors. 'HMRC was stretched before Brexit.'

What will happen to AEO?

It is unclear whether the mutual recognition benefits of authorised economic operator ('AEO') status will be maintained after Brexit, but the kitemark – which demonstrates that the trader has achieved World Customs Organisation ('WCO') standards in customs and security – is being pushed as a 'necessity' by organisations such as the Chartered Institute of Logistics and Transport ('CILT') and others.

'AEO is recognised in many countries outside the EU, including China, Japan and the USA, and is being actively supported and encouraged by the World Trade Organisation so we can expect it to be an integral part of any post-Brexit scenario,' says Roy Baker, Director of UK freight forwarder, International Forwarding Ltd, in a Brexit briefing to its customers.

Are other Member States prepared for Brexit?

France, Germany and the Netherlands are the UK's top trading partners in the EU. In the current climate of uncertainty, are exporters from these countries adequately resourced and prepared?

'BAFA [the German federal export control agency] in particular is

News feature: Brexit

perceived as being well resourced,' says Salzmann. 'The problem is the lack of visibility into arrangements of other Member States. We do not know whether there are the resources in export licensing to cope with the uplift in requirements.'

The UK is the Netherlands' second-largest export market after Germany, the recipient of mobile phones and fresh produce such as onions, meat and flowers. An Organisation for Economic Cooperation and Development ('OECD') study found that Dutch exports to the UK could drop by 17% in the event of a no-deal scenario.

'It is not clear what will happen with customs-related affairs after 29 March,' says Rick van 't Hullenaar, international trade partner at De Brauw Blackstone Westbroek in Amsterdam. 'In the Netherlands, there is heavy trade with the UK, so companies will count the commercial cost as there will be a slowdown in the logistics process that will, in turn, affect the supply chain following 29 March.'

Domestic companies are not prepared in a manner that satisfies the Dutch government, he says. A survey by the Netherlands Chamber of Commerce ('KVK') in October last year of businesses trading with the UK indicated that only 15% considered themselves to be well prepared, 46% 'somewhat' prepared and 39% were not prepared at all. 'Impact unclear, many entrepreneurs unprepared', was the conclusion of the report.

The elephantine transposition of EU secondary regulation into UK domestic law through the European Union (Withdrawal) Act 2018 covered some critical concerns for UK exporters such as the status of the Registration, Evaluation and Authorisation of Chemicals (the 'REACH' regulations) in ensuring immediate continuity post-Brexit.

The Irish government is in turn preparing a 90-page omnibus 'hard Brexit' bill, which aims to secure issues in question such as the common travel area, reciprocal healthcare, taxation and rail and bus services.

'The Bill will get bigger as the weeks go on,' says John Menton, a commercial partner with a tech specialism at Dublin firm Arthur Cox. 'The Irish government has said it is not working on anything else apart from Brexit.'

As home to many US multinationals – including Apple – which export

Unknowns and OGELs – the new UK licence for exports to the European Union

In early February, the United Kingdom's Joint Export Control Unit ('ECJU') published an open general export licence ('OGEL') which will come into force on 29 March if the UK fails to reach a deal regarding customs and trade with the European Union prior to that date. It is intended to cover exports to EU Member States.

The ECJU's notice to exporters says that the 'overall framework of controls of dual-use exports would not change, but there would be changes to some licensing requirements:

- The movement of dual-use items from the UK to the EU would require an export licence. This is not currently the case and these movements would, therefore, need to be licensed in the same way as for non-EU destinations.
- Extant export licences issued in the UK would no longer be valid for exporting dual-use items from EU Member States. A new licence, issued by an EU Member State, would be required.
- Extant export licences issued by the 27 EU countries would no longer be valid for exporting dual-use items from the UK. A new licence, issued by the UK, would be required.'

The ECJU says that to understand what controls would apply, 'licensing provisions in current legislation for a "third country" (a non-EU country) can be taken as a guide to the licensing provisions for exports to EU countries in the case of a "no deal" scenario.'

But while any guidance is welcome, there's still scope for confusion – and inadvertent non-compliance – for UK exporters. It is apparent that a number of companies have registered for the OGEL export of dual-use goods to EU Members and have received acknowledgement of their registration. But there are concerns about processes and administration.

In place of sending goods to the EU with a statement about Article 22 (10) of Council Reg (EC) 428/2009 on the invoice (as currently required), it will be necessary to ensure that the Single Administrative Document ('SAD') is completed correctly, quoting the OGEL in Box 44 of the export entry.

It will also be necessary for them to receive documentary evidence from the freight companies that they use in order that it can be used for audit purposes. (It should be noted that this is increasingly difficult now, in the case of third-country exports on account of the increase in the number of declarations and HMRC 'easements' – see for example: https://www.gov.uk/guidance/register-for-simplified-import-procedures-if-the-uk-leaves-the-eu-without-a-deal#what-transitional-simplified-procedures-are

For the moment, it should be assumed that the OGEL will be audited in the same way as other OGELs, although it seems that no end-user undertaking or consignee will be required (though the exporter will have to maintain records in line with Article 29 of the Export Control Order.)

One practical issue related to the above: How do you know you are meeting the conditions of the OGEL if you don't possess a form of end-user undertaking? Amongst the exclusions listed in the OGEL is the following:

'If the exporter knows that the final destination of the items concerned is outside [the European Union] and no processing or working is to be performed in a destination listed in Schedule 2, unless the direct export to the final destination would be permitted under a retained general authorisation, an open general export licence, or an individual export licence granted by the Secretary of State to the exporter,' (the licence does not authorise the export).

But it isn't clear what the ECJU will be expecting to see with regard to recordkeeping for the purposes of audit. For the moment, top of the list concerns must be:

- Will the trader (exporter) know to provide the export licence details to the freight forwarder?
- Will the freight forwarder know to input the licence in Box 44 of the export declaration?
- Will the goods be 'arrived' on CHIEF (e.g., presented to UK Customs for examination of the goods/licence)?
- Will the goods be 'departed' on CHIEF (official evidence of export)?

If one of the above procedures isn't carried out, then the exporter has committed a criminal offence.

Courtesy of Sandra Strong, Steve Berry and Bernard O'Connor, Strong & Herd
www.strongandherd.co.uk

News feature: Brexit

technology from Irish subsidiaries to the UK and beyond, the EU's December announcement that the UK will be added to the UGEA authorisation was met with relief. 'The addition of the UK to UGEA001 will solve our problems for the tech industry, but there is still the major impact on food producers to consider,' says Menton.

What about sanctions?

The UK's Sanctions and Anti-Money Laundering Act, which received royal assent in June 2018, creates a new domestic framework to enable the UK to impose and enforce sanctions regimes after Brexit. On 1 February 2019, the government published guidance on its expected sanctions policy in the event of no deal, which stated the UK would work with the EU and other international partners on sanctions 'where this is in our mutual interest'.

'The latest technical notice on sanctions in the event of a no-deal Brexit indicates that the sanctions policy of the EU and UK may diverge in the future,' says Salzmann.

At a time when the gap has widened between the US and the EU on sanctions policy towards Iran, with the US exiting the Joint Comprehensive Plan of Action ('JCPOA') and re-imposing nuclear sanctions, divergence at a national level creates a new variable and arguably could weaken international sanctions enforcement.

There is also a question mark over whether the UK will continue to participate in bodies overseeing the monitoring and development of export control and anti-proliferation such as the EU Dual-Use Working Party and the EU WMD Monitoring Unit. As a recent Project Alpha report concluded: '[E]nd use controls are reliant on collaborative information which is hard to achieve without EU-wide consistency.'

'In terms of information sharing, there is certainly the possibility of divergence,' says van 't Hullenaar. 'We are losing, at least in the way it is currently structured, a high-quality contributor of intelligence to the EU.'

What should exporters have in place – the very basics

Be prepared. Although the 'to do' list for Brexit is inexhaustible, there are a few essentials that should be put into effect: 'Companies need to look long and hard at their supply chains,' says Salzmann. 'They need to consider eventualities such as what would happen if they ran out of paint and it is sourced in Germany, for example.'

van 't Hullenaar notes: 'Establish which party is liable for import duties in case they will be levied. In terms of dual-use items, assess whether the item can be exported under the amended UGEA which is being proposed, or its UK counterpart, the OGEL. In more general terms, train staff, familiarise yourself with your compliance framework and be prepared to amend it, and monitor developments closely.'

Other precautions, suggest lawyers, include gaining AEO status and – if not already done – making an inventory of stock and making sure there is adequate stock in place to cover unexpected delay; obtaining an EORI number; accessing updates through the HMRC's Partnership Pack and arranging for 'pre-cleared' loads at customs after 29 March.

Time to get on with it?

IRELAND

Ireland: BREXIT and the export of dual-use goods from Ireland

By John Menton and Ciara Anderson, Arthur Cox

www.arthurcox.com

In the European Union, the export of dual-use goods is controlled by the Dual-Use Regulation (Council Regulation (EC) No 428/2009) (as amended) ('Dual-Use Regulation'). Entities that export any of the categories of goods or technologies listed in the annexes to the Dual-Use Regulation (as updated from time to time) must apply for authorisation from the Department of Business, Enterprise and Innovation ('DBEI') unless they qualify for one of the exemptions contained in the Dual-Use Regulation.

'Export' only refers to goods sent to a destination outside of the EU customs territory. For the transfer of dual-use goods within the EU customs territory, no authorisation is required (with some limited exceptions). If Brexit results in the UK leaving the EU customs territory then this exemption will no longer apply to dual-use exports from Ireland to the UK.

The requirement to apply for and receive authorisation for export of certain goods creates a cost of trade particularly if goods are exported in high volume to particular countries. In order to ease the barriers to trade, it is possible to utilise a Union general export authorisation ('UGEA') which covers exports of certain goods to certain countries. UGEA Category 001 covers the export of most goods set out in Annex 1 of the Dual-Use Regulation to eight countries: Australia, Canada, Japan, New Zealand, Norway, Switzerland (including Liechtenstein) and the United States of America.

If the UK does leave the EU on 29 March 2019 with no withdrawal agreement in place, the UK will become a 'third country' for the purposes of the Dual-Use Regulation. If this occurs, dual-use goods exported from Ireland to the UK will be subject to the Dual-Use Regulation and will require authorisation from the DBEI to export.

To avoid this consequence in a no-deal Brexit scenario, the European Commission has published a draft regulation which would include the UK on the list of countries which are subject to UGEA Category 001. In the event the EU approval process for the draft regulation is delayed, the DBEI has now stated that it will also introduce a national measure equivalent to a UGEA in Ireland. The DBEI issued a notice to exporters on 16 January 2019 and it recommends that any company currently exporting subject to a UGEA, and which is currently exporting or planning to export dual-use goods to the UK, notify the Export Licensing Unit of the DBEI now in order to avoid any potential processing delays. Furthermore, even if a company does not currently operate under a UGEA but is currently exporting or planning to export dual-use goods to the UK, it should also contact the Export Licensing Unit of the DBEI.

LUXEMBOURG

Luxembourg's new single export control regulation brings comprehensive change

By Yvo Amar, Wladimiroff Advocaten N.V.

www.wlaws.com

On 14 December 2018, Luxembourg's new export control law and regulation were published in the Grand Duchy's official journal. The regulation implements an act dated 27 June 2018, which provides for a new framework for the implementation of UN and EU sanctions regulations and the EU Dual-Use Regulation in Luxembourg.

Both the act and the regulation focus, in particular, on the export of goods. However, except in so far as to the extent it covers financial services as auxiliary services in relation to, for example, the export of military items, the act does not provide for specific rules on the risks of financing proliferation or other financial risks in this context.

Prior to 2018, Luxembourg did have an export control regime, but this was

based on many separate regulations. These have now been annulled and incorporated into one new Act and Regulation.

In essence, the Act and the Regulation provide the framework for the regulation of export authorisations in relation to dual-use items and military items and related services and set prohibitions in relation to UN and EU sanctions. The fact that it also covers UN sanctions is interesting and in that regard is similar to Belgium.

Whereas in the Netherlands and in most of the EU, UNSC regulations require prior implementation into EU regulations to become effective, in Belgium and Luxembourg, they have direct application, regardless of their implementation into EU legislation.

The Luxembourg Regulation further elaborates on the framework set by the Act, even creating a new customs Office in Luxembourg responsible for the application of the export control system described in the Act.

The Office is to operate under the responsibility of the Luxembourg Minister of Commerce and will be responsible for, among others, the preparation of export authorisations, the provision of information to the public, the prevention of proliferation, etc.

Unusually, the Regulation is detailed on the treatment of export authorisation applications and provides a long list of annexes, including application forms and the form of authorisations. Annex 1 provides for a complete overview of all consequences of the UN and EU sanctions per sanctioned country.

The Regulation ends by describing the obligations of officials within the Office, the numbers that should be employed, their required competences and the number of hours they must be trained on each particular subject (six hours on criminal law, four hours on criminal procedural law and four hours on proliferation studies).

See the act and regulation at:
http://legilux.public.lu/eli/etat/leg/loi/2018/06/27/a603/jo

http://legilux.public.lu/eli/etat/leg/rgd/2018/12/14/a1158/jo

USA

US expands Venezuela sanctions, targets PdVSA

By Richard Burke, Nicole Erb, Claire A. DeLelle, Kristina Zissis, Cristina Brayton-Lewis, Emily Holland, Sandra Jorgensen and Margaret Spicer, White & Case

www.whitecase.com

On 28 January 2019, the Department of the Treasury's Office of Foreign Assets Control ('OFAC') designated Petróleos de Venezuela, S.A. (PdVSA) on the List of Specially Designated Nationals and Blocked Persons ('SDN List').

PdVSA is designated pursuant to Executive Order ('EO') 13850 for operating in the oil sector of the Venezuelan economy.[1]

For parties designated on the SDN List such as PdVSA, all of their property and interests in property located in the United States or within the possession or control of a US person,[2] wherever located, are blocked and may not be dealt in. Any entity in which one or more SDNs directly or indirectly holds a 50% or greater ownership interest in the aggregate is itself deemed blocked by operation of law. US persons – including foreign branches of US companies – may not engage in any dealings, directly or indirectly, with blocked persons. Provision of goods, services, or support to blocked parties may be grounds for potential future designation.

OFAC has issued nine general licences to mitigate the effects of the designation in specific circumstances set forth in each General Licence, two of which have been replaced and superseded by new licences. These General Licences also generally establish that transactions and activity otherwise prohibited by previous Venezuela-related executive orders continue to be prohibited. It is important, therefore, for companies to make sure they still consider the prior executive orders and OFAC guidance regarding Venezuela when they analyse the General Licences to determine whether certain activity is permitted or prohibited.

Additionally, on 25 January 2019, President Trump signed EO 13857 entitled 'Taking Additional Steps to Address the National Emergency with Respect to Venezuela' to expand the definition of the term 'Government of Venezuela' to include persons that have acted, or have purported to act, on behalf of the government of Venezuela, including members of the Maduro regime.[3]

The designation of PdVSA follows a determination by US Treasury Secretary Steven Mnuchin that persons operating in the oil sector of the Venezuelan economy may be subject to sanctions under EO 13850.[4] OFAC issued guidance stating that PdVSA may be delisted through 'expeditious transfer of control to [US-recognised interim president Juan Guaidó] or a subsequent, democratically elected government.'[5] OFAC has issued 13 frequently asked questions ('FAQs') and amended five of those FAQs in two stages in connection with the PdVSA designation and related general licences.[6]

On 29 January 2019, the Department of State also announced that it certified the authority of Mr. Guaidó to receive and control certain property in accounts of the government of Venezuela or the Central Bank of

Venezuela held by the Federal Reserve Bank of New York or any other US-insured bank.[7]

General Licences

OFAC has issued nine General Licences providing temporary relief from the new sanctions.

Two of the General Licences have been replaced and superseded by new General Licences (GLs 3C and 9B), and OFAC has issued FAQs describing the scope of these amendments that modify the conditions under which certain transactions are authorised.

The authorisations, as amended, are described in the chart below.

Licence	Authorises	Expiration	Restrictions
GL 3C: Authorizing Transactions Related to, Provision of Financing for, and Other Dealings in Certain Bonds[8]	Transactions related to, the provision of financing for, and other dealings in bonds (enumerated in an annex, the "GL 3C Bonds") that would otherwise be prohibited, provided any divestment or transfer of, or facilitation of divestment or transfer of holdings in such bonds is to a non-US person.[9] (absent authorisation from OFAC).[10] Transactions and activities ordinarily incident and necessary to the wind down of financial contracts or other agreements entered into prior to 4:00 p.m. eastern standard time on 1 February 2019, involving or linked to the GL 3C Bonds.[11] Transactions related to, the provision of financing for, and other dealings in bonds issued both (i) prior to 25 August 2017 and (ii) by US person entities owned or controlled, directly or indirectly by the government of Venezuela, other than Nynas AB, PDV Holding, Inc. (PDVH), CITGO, and any of their subsidiaries.[12]	Financial contracts wind down: 3 March 2019	Does not authorise any transaction that is otherwise prohibited under pre-existing sanctions. Does not authorise US persons to purchase or invest in, or to facilitate the purchase of or investment in, directly or indirectly, bonds issued by the government of Venezuela prior to 25 August 2017 (including the GL 3C Bonds), other than purchases of or investments in GL 3C Bonds ordinarily incident and necessary to the divestment or transfer of holdings in GL 3C Bonds.
GL 7: Authorizing Certain Activities Involving PDV Holding, Inc. and CITGO Holding, Inc.[13]	Activities involving PDVH, CITGO, and their subsidiaries where the only PdVSA entities involved are PDVH, CITGO, or their subsidiaries. PDVH, CITGO, and their subsidiaries to engage in all transactions ordinarily incident and necessary to the purchase and importation of petroleum and petroleum products from PdVSA and any entity in which PdVSA owns, directly or indirectly, a 50% or greater interest.[14]	27 July 2019 28 April 2019	Does not authorise exportation or reexportation of goods, services, or technology by US persons or from the United States, to PdVSA or any entity owned 50% or greater, directly or indirectly by PdVSA other than PDVH, CITGO,and their subsidiaries. Does not authorise such exports or reexports to other blocked persons.
GL 8: Authorizing Transactions Involving PDVSA Prohibited by Executive Order 13850 for Certain Entities Operating in Venezuela[15]	Chevron Corporation, Haliburton, Schlumberger Limited, Baker Hughes (a GE Company), and Weatherford International PLC and their respective subsidiaries are authorised to carry out all transactions and activities ordinarily incident and necessary to operations in Venezuela involving PdVSA and any entity which PdVSA owns 50% or greater, directly or indirectly.	27 July 2019	Does not authorise the exportation or reexportation of diluents from the United States to Venezuela.

continues

Licence	Authorises	Expiration	Restrictions
GL9B: Authorizing Transactions Related to Dealings in Certain Securities[16]	Transactions and activities ordinarily incident and necessary to dealings in any debt (including, but not limited to, bonds enumerated in an annex)[17] or any equity in PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly, issued prior to 25 August 2017 (collectively 'PdVSA securities'), provided any divestment or transfer of, or facilitation therein, of holdings in such securities is to a non-US person18 (absent authorisation from OFAC).[19] Transactions and activities ordinarily incident and necessary to the wind down of financial contracts or other agreements entered into prior to 4:00 p.m. eastern standard time on 28 January 2019, involving or linked to PdVSA securities issued prior to 25 August 2017.[20] Transactions and activities ordinarily incident and necessary to dealings in bonds issued prior to 25 August 2017 by PDV Holdings, CITGO, Nynas AB, and their subsidiaries.[21]	Wind down activities: 11 March 2019 Others: None	Does not authorise US persons (i) to sell or to facilitate the sale of, PdVSA securities to, directly or indirectly, any blocked person, or (ii) to purchase or invest in, or to facilitate the purchase of or investment in, directly or indirectly, PdVSA securities, other than purchases of or investments in PdVSA securities (including settlement of purchases or sales pending on 28 January 2019) ordinarily incident and necessary to the divestment or transfer of holdings in PdVSA securities.
GL 10: Authorizing the Purchase in Venezuela of Gasoline from PDVSA[22]	Purchase of refined petroleum products by US persons in Venezuela for personal, commercial, or humanitarian uses from PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly.	None	Does not authorise the commercial resale, transfer, exportation, or reexportation of refined petroleum products.
GL 11: Authorizing Certain Activities Necessary to Maintenance or Wind Down of Operations or Existing Contracts with PDVSA[23]	Transactions and activities ordinarily incident and necessary to the maintenance or wind down of operations, contracts, or other agreements involving PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly, in effect prior to 28 January 2019, by US-person employees and contractors of non-US entities located outside of the US or Venezuela. US financial institutions to reject certain funds transfers involving both (1) PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly, and (2) non-US entities located outside of the United States or Venezuela.[24]	29 March 2019	Does not authorise any transactions or dealings with ALBA de Nicaragua (ALBANISA) or entities that ALBANISA owns 50% or greater, directly or indirectly.
GL 12: Authorizing Certain Activities Necessary to Wind Down Operations or Existing Contracts with PDVSA[25]	Transactions and activities that are ordinarily incident and necessary to the purchase and importation into the United States of petroleum and petroleum products from PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly. Transactions and activities that are ordinarily incident and necessary to the wind down of operations, contracts, or other agreements – including the importation into the United States of goods, services, or technology not authorized above – involving PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly that were in effect prior to 28 January 2019.	28 April 2019 27 February 2019	Does not authorise: (1) the divestiture or transfer of any debt, equity, or other holdings in, to, or for the benefit of PdVSA or entities that PdVSA owns 50% or greater, directly or indirectly; (2) the exportation or reexportation of diluents from the United States to Venezuela, PdVSA, or entities that PdVSA owns 50% or greater, directly or indirectly; or (3) any transactions or dealings with ALBANISA or entities that ALBANISA owns 50% or greater, directly or indirectly.

continues

Licence	Authorises	Expiration	Restrictions
GL 13: Authorizing Certain Activities Involving Nynas AB[26]	Transactions and activities where the only PdVSA entities involved are Nynas AB or its subsidiaries.[27]	27 July 2019	Does not authorise the export or reexport of goods, services, or technology, directly or indirectly, by US persons or from the United States to PdVSA, other than Nynas AB or its subsidiaries, or to any other blocked person.
GL 14: Official Business of the United States Government[28]	Transactions that are for the conduct of the official business of the United States Government by employees, grantees, or the contractors thereof.	None	

Venezuela files WTO challenge to US sanctions measures

On 8 January 2019, the World Trade Organization ('WTO') announced that Venezuela initiated a dispute in the WTO against the United States regarding US sanctions measures targeting Venezuela by requesting dispute consultations on 28 December 2018.[29] The parties have 60 days from the date of the request to attempt to resolve the dispute before it will proceed to adjudication. In its request for consultations, Venezuela claims that measures imposed under certain US sanctions-related statutes, regulations, and EOs relating to goods of Venezuelan origin, imports of gold from Venezuela, the liquidity of Venezuela's public debt, transactions in government-backed cryptocurrency, and the supply and consumption of services by certain Venezuelan nationals placed on the SDN List are coercive trade-restrictive measures in violation of the General Agreement on Tariffs and Trade 1994 ('GATT') and the General Agreement on Trade in Services ('GATS'). The dispute is currently in the consultation phase.[30]

Parties that conduct business with Venezuela should be aware of the US sanctions currently in place against Venezuela. Non-compliance could result in severe penalties for sanctions violations.

Links and notes

[1] The OFAC designation announcement is available at https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190128.aspx. E.O. 13850 was signed by President Trump on 1 November 2018, and is available at https://www.govinfo.gov/content/pkg/FR-2018-11-02/pdf/2018-24254.pdf.

[2] US person is defined to include US citizens and permanent resident aliens, wherever located, entities organised under US law (including foreign branches), and individuals and entities located in the United States.

[3] The EO is available at https://www.whitehouse.gov/presidential-actions/executive-order-taking-additional-steps-address-national-emergency-respect-venezuela/. OFAC published a new FAQ on this EO, available at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#649.

[4] See OFAC press release, available at https://home.treasury.gov/news/press-releases/sm594

[5] The press statement recognising Juan Guaidó as interim President of Venezuela is available at https://www.state.gov/secretary/remarks/2019/01/288542.htm.
FAQ 660 is available at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#660.

[6] OFAC recent actions notices for these FAQs, issued 31 January (https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190131_33.aspx), 1 February (https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190201.aspx), and 11 February (https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20190211.aspx).
The 13 FAQs are at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#650 (#650 through #662).
The five amended FAQs can be found at https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#595 (#595), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#648 (#648), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#650 (#650), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#661 (#661), and https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#662 (#662).

[7] The State Department's press statement is available at https://www.state.gov/r/pa/prs/ps/2019/01/288634.htm.

[8] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl3c.pdf. GL 3C supersedes GL 3B. GL 3B, issued 1 February 2019, superseded GL 3A, which was issued on 31 January 2019. GL 3C keeps the changes that GL 3B and GL 3A implemented in superseding GL 3 of 25 August 2017, excluding Nynas AB, PDVH, CITGO Holding, Inc. and their subsidiaries from the authorisation for dealings in bonds issued prior to 24 August 2017 by US entities owned or controlled by the government of Venezuela. Dealings in bonds issued by Nynas AB, PDV Holdings, Inc., and CITGO are now provided for under GL 9B, discussed below.

[9] OFAC FAQ 650 (https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#650) articulates that if a US broker or financial institution involved in a transfer or divestment of such debt has knowledge or reason to know that the buyer is a US person, then the US broker or financial institution will be held responsible if it does not take appropriate steps to ensure the trade is not consummated (absent authorisation from OFAC), and that OFAC will consider the totality of the circumstances surrounding the processing of an unauthorised transaction in determining what, if any, enforcement action to take.

[10] OFAC FAQ 662 (https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#662) articulates that GL 3C authorises engaging in transactions related to the receipt and processing of interest or principal payments, and acting as a custodian for US and non-US persons' holdings in enumerated bonds, including acting as a custodian for a non-US person after that person has received enumerated bonds from a US person in a divestment transaction. It also includes all transactions ordinarily incident and necessary to facilitating, clearing, and settling trades of holdings in these bonds by US persons, provided such trades were placed prior to 4:00 p.m. eastern standard time on 1 February 2019.

[11] OFAC FAQ 662 also indicates this includes resolving the purchase and sale of securities, securities lending, repurchase agreements, and swaps, and derivative contracts in securities.
[12] OFAC FAQ 662 outlines what General License 3C authorises with respect to government of Venezuela debt, and the implications for US and non-US persons.
[13] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl7.pdf.
[14] GL 7 requires that payments to or for the direct or indirect benefit of blocked persons other than PDVH, CITGO, and their subsidiaries that are ordinarily incident and necessary to give effect to authorised transactions be made into a blocked, interest-bearing account in the United States.
[15] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl8.pdf.
[16] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl9b.pdf. GL 9B supersedes GL 9A of 1 February 2019, which superseded GL 9 'Authorizing Transactions Related to Dealings in Certain Debt,' which was issued on 28 January 2019. GL 9B keeps the substantive amendments of GL 9A, which added language concerning equity and Executive Order 13850. It also amended the annex.
[17] See OFAC FAQ 651 (https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#651) that certain bonds previously included in the Annex to GL 3 are now in the Annex to GL 9B.
[18] OFAC FAQ 650 (https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#650) articulates that if a US broker or financial institution involved in a transfer or divestment of such debt or equity has knowledge or reason to know that the buyer is a US person, then the US broker or financial institution will be held responsible if it does not take appropriate steps to ensure the trade is not consummated (absent authorisation from OFAC), and that OFAC will consider the totality of the circumstances surrounding the processing of an unauthorised transaction in determining what, if any, enforcement action to take.
[19] OFAC FAQ 661 (https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#661) clarifies GL 9B's authorizations with respect to PdVSA securities and the implications for US and non-US persons. This authorisation includes facilitating, clearing, and settling transactions to divest to a non-US person, including on behalf of a US person (which includes engaging in transactions related to the receipt and processing of interest or principal payments, and acting as a custodian for US and non-US persons' holdings in PdVSA securities, including acting as a custodian for a non-US person after that person has received PdVSA securities from a US person in a divestment transaction). It also includes all transactions and activities ordinarily incident and necessary therein, provided trades were placed prior to 4:00 p.m. eastern standard time on January 28, 2019.
[20] OFAC FAQ 661 also indicates that this authorisation allows the wind down of certain financial contracts and agreements entered into prior to the imposition of blocking sanctions on PdVSA that involve or are linked to PdVSA securities, including resolving the purchase and sale of securities, securities lending, repurchase agreements, and swaps and derivative contracts in securities.
[21] OFAQ FAQ 661 articulates that US persons may continue to hold their interests in PdVSA securities but are subject to certain restrictions concerning the sale of those interests on the secondary market. It clarifies that GL 9B does not generally authorise US persons to purchase or acquire new interests in PdVSA securities (absent authorisation from OFAC) but that US persons may purchase or invest in PdVSA securities where such transactions are ordinarily incident and necessary to the divestment and transfer of holdings in PdVSA securities. Finally, non-US persons may continue dealing in PdVSA securities, but to the extent such transactions involve US persons or the US financial system the transactions must comply with GL 9B and may not involve unauthorised sales of such securities to US persons.
[22] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl10.pdf.
[23] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl11.pdf.
[24] GL 11 authorises US financial institutions to reject fund transfers that originate and terminate outside the United States and for which neither the originator nor the beneficiary is a US person, and the funds are not destined for a blocked account on the books of a US person.
[25] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl12.pdf. GL 12 requires that, except as authorised pursuant to GLs 7, 8, 11, and 13, payments to or for the direct or indirect benefit of blocked persons and their subsidiaries that are ordinarily incident and necessary to give effect to authorised transactions are made into a blocked, interest-bearing account in the United States.
[26] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl13.pdf.
[27] GL 13 requires that, except as authorised by GL 11, any payment to or for the direct or indirect benefit of a blocked person other than Nynas AB or its subsidiaries that is ordinarily incident and necessary to give effect to transactions authorised above that come into the possession or control of a US person must be put into a blocked, interest-bearing account located in the United States.
[28] https://www.treasury.gov/resource-center/sanctions/Programs/Documents/venezuela_gl14.pdf.
[29] The WTO news alert is at https://www.wto.org/english/news_e/news19_e/ds574rfc_08jan19_e.htm
[30] DS574: United States – Measures relating to trade in goods and services (https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds574_e.htm).

CAYMAN

PIAM: An important decision on the scope of UN and EU sanctions

By Paul McMaster QC, Paul Kennedy and Anna Snead, Appleby Global

www.applebyglobal.com

International sanctions were imposed by the United Nations in respect of Libya in 2011. The UN resolutions were given effect by the EU and in the Cayman Islands through the Libya (Restrictive Measures) (Overseas Territories) Order 2011 (as amended) ('the Order').

Article 10(4) of the Order implements an asset freeze: unless under the authority of a sanctions licence, a person shall not 'deal with' funds or economic resources which are owned, held or controlled by a person designated under the Order. It is also an offence to circumvent the Order.

Palladyne International Asset Management ('PIAM') brought claims against three Cayman Islands investment funds (the Upper Brook Funds), whose assets were frozen under the Order, and their proper directors. PIAM's primary case was that the term 'use', when properly interpreted, is wide enough, when it relates to 'funds' which are shares in a Cayman company, to cover the exercise of voting rights to appoint and/or remove directors of that company.

In the decision of *PIAM v Upper Brook (A) Ltd & Ors*, Justice Segal has held that the prohibition on 'use' of funds (in this case, shares) does not extend to cover the exercise of voting rights by a shareholder.

If PIAM's wide interpretation had been found to be correct, this would have had significant implications for the corporate governance of companies whose assets are frozen by international sanctions and would have led to perverse outcomes. If correct, a shareholder of a company would be unable to exercise any of the rights attaching to that share, without first obtaining a sanctions licence. This would have resulted in an unworkable and oppressive sanctions regime,

requiring a licence to be obtained for every matter of corporate governance, however mundane, such as changing the name of the company.

The Upper Brook Funds successfully argued that PIAM's interpretation of the prohibition on 'use' of shares would have been contrary to the plain and ordinary meaning of the legislation and inconsistent with the object and purpose of the asset freeze. The aim of the sanctions regime was to prohibit the dealing with (including 'use of') funds as financial assets. In the context of a share, this means buying it, selling it, trading in relation to it, or raising money using it as security; the prohibition is not concerned with the exercise of voting rights attached to and inherent in the ownership of the shares.

In providing helpful clarification on the prohibition of 'use' of funds, Justice Segal made the following points:

1. The term 'use' of the funds should be construed having regard to the language used in article 10(4) of the Order as a whole, and the purpose of the UN sanctions regime, which was intended to preserve the assets intact, so that they can eventually be returned to the Libyan people. The asset freeze was designed to prevent any action being taken which would make the asset (in this case, the shares) less valuable.
2. The definitions of 'funds' (as 'financial assets and benefits of every kind') and 'to deal with' in article 10(4) made clear that the sanctions legislation was concerned with the 'use' of the share in its character as a financial asset. Use of the funds must be taken as referring to an activity in which the funds are employed as cash/money or liquid assets; such activity is likely to involve a financial return being generated, or affect the value of the funds.
3. PIAM's wide interpretation of 'use' would significantly extend the scope of the asset freeze (as established by other prohibitions) and go beyond what is necessary to achieve the purpose of the freeze. Clear and explicit language would have been needed to justify this interpretation, particularly given the serious consequences of a breach. Furthermore, if it had been intended that the UN Sanctions Committee would review the suitability of proposed new directors, the UN resolutions would have said so and the Order would have made provision for this in clear terms.

Justice Segal also rejected PIAM's alternative argument that the exercise of voting rights by the shareholders to remove and/or appoint new directors made a change that would 'enable use' or 'allow access' to the underlying assets of the Cayman funds. The particular issue at hand was whether votes to remove and replace directors of the Upper Brook Funds had involved breaches of international sanctions.

The funds had received some USD 700,000,000 of investment of Libyan sovereign wealth. In addition to arguing that shares had been used in breach of sanctions, PIAM argued that the shares had been unlawfully dealt with by making a change that would allow access to the underlying investments or enable their use. Both of these arguments were rejected on the basis that a mere change of control over the company by replacing its directors neither allowed access to the underlying investments or enabled their use.

This is the first major decision in the Cayman Islands on international sanctions. However, its significance is not limited to Cayman Islands law and the interpretation of the prohibition on 'use' in article 10 of the Order. Justice Segal found that the international sanctions regime (UN, EU, UK and Cayman) should be read as a single harmonious code. This decision will therefore be highly relevant to the interpretation of UN and EU sanctions globally as well as UK domestic legislation implementing international sanctions.

Appleby (Cayman) Ltd represented the Upper Brook Funds and Dinah Rose QC appeared for them as counsel at trial.

Events, dear reader, events

Regardless of whether Harold Macmillan ever actually said that the things most likely to blow governments off course were 'Events, dear boy, events,' there are certainly enough of them to go around for administrations the world over to blame for their own failings.

Indeed, Macmillan's successor to the prime ministership has found that governments themselves are perfectly able to become the very event that blows itself off course – a kind of perversion of the mantra of the positive thinking brigade: 'Be the change that you [don't] want to be…'

As at writing time, Theresa May is about to announce something important relating to Brexit; the Iranian Foreign Minister is resigning; Nicolas Maduro is not resigning (and nor is Theresa May); Kim Jong-un is stepping off a train at Hanoi station to rekindle his bromance with the man who once called him Little Rocket Man; and India has attacked 'terrorist' positions on the Pakistan side of the Line of Control in Kashmir.

All these things may feel far removed from the day-to-day jobs of compliance professionals and lawyers

As at writing time, Theresa May is about to announce something important relating to Brexit.

but they're not. For events (dear reader), not only blow governments off course – they also generate enormous amounts of paperwork.

Honda is a brand which has been in the news a lot recently. In the UK, it was the company's announcement that it would be closing its operations in Swindon in 2022 with the loss of over 3,000 jobs, that hit the headlines. It refused to attribute the decision to Brexit, instead pointing the finger at 'a number of contributory factors' (amongst them, a phasing out of cars as we know them in favour of the next generation of battery-powered run-arounds).

But from a strictly compliance perspective, it was the company's settlement with the US DoJ, to the tune of a not-crippling $44,000, that piqued my interest. The money was paid to the Immigration and Employee Rights section. The company's mis-step was an attempt to restrict hiring for ITAR-related roles to 'lawful permanent residents and/or U.S. citizens' and not extending the offer to the broader definition of 'US Person' which includes refugees and asylees.

There is, of course, always a tendency – especially in an environment where national security considerations are heightened – to over-comply. But doing so, of course, comes at the risk of overstepping other bounds.

Tom Blass, February 2019
TNB@worldecr.com

INSTEX. Will it work?

Is the new three-state SPV for facilitating Iran trade a step in the right direction, or merely an expression of political will?

The creation of INSTEX – 'Instrument for Supporting Trade Exchanges' – has been much covered in the press. Designed by three [current] EU Member States to provide a means by which companies can conduct legitimate trade – for now, the sale of food, medicine and medical devices, though possibly expanding that in the future – with Iran and receive payment for their exports, the question is: Will it work? *WorldECR* asked two sanctions consultants, Fabian Jahn, a rechtsanswalt in Munich, and Aleksi Pursiainen of Solid Plan consulting in Helsinki, to each provide a perspective...

Fabian A. Jahn, rechtsanswalt, Munich
www.der-rechtsanwalt.eu

In their dealings with Iran, EU businesses are faced with challenges and consequences even in entirely compliant transactions – for example, and as has been often noted, persuading banks to make legal transfers from Iran to their accounts can be extremely problematic. Thus, even companies that continue to do business with Iran despite the obvious hurdles face the problem of getting their bills paid – a problem made even more difficult by the US withdrawal from the Joint Comprehensive Plan of Action ('JCPOA') and its insistence that it will continue to enforce secondary sanctions strongly.

In an initiative undertaken to attempt to address this issue, Germany, France and the UK decided to adopt the model already under consideration in Switzerland. In late January 2019, the foreign ministers of the three countries announced that they aim to establish a private legal entity, called INSTEX: the 'Instrument for Supporting Trade Exchanges'.

INSTEX is a private entity, founded as a French SAS (plc). It was registered

on 31 January 2019 in Paris. It is headed by former Commerzbank manager Per Fischer. The intention of this special purpose vehicle ('SPV') is that it should help companies in France, Germany and the UK receive payment for exports to Iran.

It works according to the offset business principle. EU importers pay money into INSTEX; EU exporters are paid from the funds placed into INSTEX but receive no funds directly from Iran.

Before it can function, Iran must also establish a correlating SPV, but, as at time of writing, it is unclear as to whether it is able to do so. And, as a requirement of the governments that initiated INSTEX, Iran needs to reform its AML regime.

Further, it's unclear at time of writing whether banks are prepared to accept and provide remittances from/to it.

And there is still another problem. For INSTEX to be able to pay EU exporters, there must be enough imports into the EU from Iran – and there is no certainty that that will be the case.

Currently there is a significant trade deficit between Iran and the EU. According to data from German trade agency GTAI, imports of non-petrochemical and non-oil products from Iran into the EU were worth 800 million euros in 2017. EU exports amounted to 10.8 billion euros. EU exports of humanitarian goods alone amounted to 1.9 billion (500 million euros' worth being from Germany). Given those figures, anything like parity looks unlikely.

Switzerland wants to establish a SPV, too, through which shipments of humanitarian goods to Iran should be settled. Switzerland is seeking US consent for its SPV. It is not known whether Germany, France and UK will do the same. But, as with Switzerland, the EU INSTEX is also intended to be used initially for the shipment of humanitarian goods.

For European companies – especially those without interests in the US market and without US connections – INSTEX could be an option, particularly for those that export humanitarian goods, like agricultural goods and commodities relevant for the health sector. There are estimates that about 80% of Germany's exports to Iran are humanitarian ones.

There are rumours that Turkish President Erdogan is considering a Turkish SPV to bypass the international bank-standard SWIFT and so keep trade channels open.

Nevertheless, risks remain. INSTEX is clearly indicative of a stance at odds with US sanctions policy, and the US government has already said it would not accept anything that it interpreted as an evasion of the Iran sanctions regime – which may explain a lack of euphoria on the part of European businesses at the announcement of INSTEX. The German industry association, BDI stated in a brief press release that it welcomed INSTEX, yet expressed scepticism about its ability to balance the books. At the same time, it criticised 'overcompliance' by banks in the EU.

Aleksi Pursianen, SolidPlan, Helsinki
https://solidplan.fi/

While the JCPOA is imperfect, it still represents our best chance of curbing Iran's nuclear ambitions, a development which would have

unpredictable, but almost certainly profound and deeply negative consequences in the region and globally. The JCPOA does not address all aspects of Iran's behaviour that we should be concerned about, but it is immensely unlikely that any single deal available would.

From this perspective, the idea of a special purpose vehicle is laudable. The JCPOA has a chance of survival only as long as it remains politically defensible in Iran, where the bitter taste of perceived capitulation to Western bullying was made sweeter by the promise of rising living standards, improved infrastructure, and access to Western goodies for all.

The moment it becomes clear that the Europeans will not be able to trade with Iran, that promise is revealed as hollow, leading almost certainly to a reversion to conservative and traditionalist foreign policy in Iran. Therefore, the EU is absolutely on the right track in seeking to solve the payment channel issue, a key blocking point for EU exports.

However, INSTEX comes nowhere close to providing a real solution.

Firstly, it remains unclear when the mechanism will be opened for business. At the very least, this would require Iran to establish a similar counter-mechanism in Tehran, since payments would have to be settled at that end as well. If the time it took the EU to establish its own mechanism is anything to go by, it may be a good while yet before that happens.

Even when it does, who knows what it would look like? Worryingly, unless the mechanism offers absolute transparency towards the EU, it may well end up creating an additional source of compliance risk. Imagine if after a year of trading it turns out that the Tehran end of the mechanism has all the while been effectively controlled by an Iranian financial institution subject to sanctions, or that its local managers have engaged in systematic money-laundering as part of the operation.

Secondly, while its support for trade in humanitarian goods is of course warmly welcome, the exclusion of all other trade means that the vast majority of interested European exporters will be excluded from using it. It will also mean that the overall level of trade will not satisfy the Iranian public's thirst for integration with Western markets. It may also be worthwhile to point out that trade in medicine and agricultural commodities is currently permissible under both the EU and US sanctions, meaning any bank in existence, including US banks, could legally do today what INSTEX may or may not be able to do months from today. This seems like a very complex solution to something that should not have been a problem in the first place.

Thirdly, it is not clear whether INSTEX will even solve the key issue, which is that exporters are currently unable to receive payments to their bank accounts. Sure, INSTEX may be able keep records of the debits and credits of exporters and importers, but sooner or later, actual funds will need to be transferred to an actual bank.

Banks are not currently accepting payments originating from Iranian trade, because they assess the compliance costs and risks too high: What if the exporter messed up its due diligence, or what if the bank's own internal controls turn out to be inadequate under some new and innovative OFAC interpretation? But adding INSTEX and its Iranian counterpart to the transaction will certainly not lower the risk of a compliance breach somewhere along the way. If anything, such a non-traditional and untested mechanism is all but certain to be more exposed to compliance risk than traditional banking channels, guarded as they are by a battallion of compliance officers armed with automated screening tools and artificial intelligence solutions.

Worryingly, unless the mechanism offers absolute transparency towards the EU, it may well end up creating an additional source of compliance risk.

So, why would a bank accept a payment from INSTEX? If the underlying transaction was inconsistent with US sanctions, the bank would still be on the hook for having facilitated a prohibited transaction.

Finally, on a lighter note, I find it amusing that INSTEX appears to have been purposefully designed so that it will not run afoul of any US extraterritorial sanctions. This means that the two things the EU has so far been able to do to protect European exporters is to threaten them with penalties if they comply with secondary sanctions (the Blocking Regulation) and to develop a payment channel carefully crafted so that it does.

All of this notwithstanding, INSTEX is a positive development deserving of the support of European business. Right now, however, it is not so much a small step in the right direction as it is a public statement of a firm determination to take a small step in the right direction later on, circumstances permitting.

Trump-Kim Part II: where to now?

Best not to expect too much positive to come out of the presidents' much-anticipated Vietnam summit, writes Shea Cotton.

In his 2019 State of the Union Address, President Trump confirmed there would be a second summit between him and Kim Jong-un, to be held in Vietnam at the end of February. Both sides are looking to build on what were largely symbolic gains from their first face-to-face meeting. So, what has happened since the first summit and what will Kim Jong-un's goals be for this one?

At the first summit, Trump and Kim signed a 400-word joint statement saying each would work to establish a permanent 'peace regime' and that North Korea would commit to working towards 'denuclearisation of the Korean Peninsula'.[1] Unfortunately, both these phrases are exceptionally vague, denuclearisation especially. To the United States, denuclearisation of the Korean Peninsula means the complete nuclear disarmament of North Korea. For North Korea, the term means something more akin to 'I'll get rid of my nuclear weapons when either the US stops supporting South Korea or gets rid of its nuclear weapons too'.

A series of meetings at the working level and ministerial level has followed the first summit. Secretary of State Mike Pompeo traveled to Pyongyang on 26 September[2] and on 7 October.[3] Additionally, Kim Jong-un met with South Korean President Moon Jae-in. Unfortunately, these diplomatic interactions appear to have resulted in little more than symbolic gestures and arrangements for a second summit.

Several of these symbolic gestures are worth discussing to understand what is on the table and what is not. At the Kim and Moon meeting, North Korea stated it would dismantle rocket test and launch facilities at Sohae Satellite Launching Station.[4] Satellite imagery subsequently confirmed that several parts of the facility, such as an engine test stand and fuel/oxidiser bunkers, were being taken down and removed.[5] Additionally, North Korea also stated it is willing to dismantle its 5 MWe plutonium-producing nuclear reactor at Yongbyon (provided the US takes undefined 'corresponding measures' in return). While each sounds promising, their importance in North Korea's missile and nuclear programmes, respectively, is minimal. North Korea has largely shifted away from using fixed launch sites (like the kind used at Sohae) to mobile platforms that can be set up and launched from quickly. Similarly, Yongbyon is believed to be only one of several nuclear facilities scattered around North Korea.

The prospects for a productive summit are dim.

Recently, Steve Biegun, the US Special Representative for North Korea – rather dubiously – expanded on these claims saying that North Korean officials privately told him they were willing to dismantle all plutonium and uranium enrichment facilities.[6] Biegun also stated that the US will be seeking to get (and believes the North Koreans will likely give) a comprehensive declaration on all North Korea's weapons of mass destruction. If Beigun's views are widely held within the administration, then all are in for a shock. North Korea has never stated it is willing to give up its nuclear weapons. Nor is the regime likely to provide a full declaration of its WMD and missile facilities, much less its nuclear facilities. To the contrary, Kim Jong-un stated at the start of 2018 that North Korea would begin mass-producing nuclear weapons and the missiles to carry them and several reports suggest it is doing exactly that.[7]

Summit's gotta give

The prospects for a productive summit are dim, given the apparent distance between what each side wants and the likely outcome will be more symbolic gestures. In exchange, for the lifting of some sanctions or a peace declaration stating that the Korean War is officially over, North Korea may be willing to dismantle its reactor at Yongbyon. This brings North Korea to a key goal: normalising relations with the US and legitimising its possession of nuclear weapons. Meanwhile, the trade – removing the reactor and dismantling missile testing sites – will do little to move North Korea towards eliminating its nuclear weapons.

The worst-case scenario for this summit is that Trump realises North Korea will not give up its weapons and feels deceived. This could trigger a breakdown in diplomacy entirely and see a quick return to the fiery rhetoric and missile/nuclear testing. I personally don't see this as likely as it would require Trump to admit he has failed as a dealmaker. Similarly, North Korea will likely be able to keep Trump interested with further symbolic gestures like dismantling missile test sites or at the very least, statements saying they would be interested in such actions in exchange for further normalising steps from the US.

This is a shame. The current thaw in tensions is welcome compared to the tensions of two years ago. However, without meaningful diplomacy this thaw will likely be temporary, and these negotiations could poison the potential for meaningful ones in the future.

Shea Cotton is a Research Associate at the James Martin Center for Nonproliferation Studies in Washington, DC .

scotton@miis.edu

Links and notes

1 https://www.whitehouse.gov/briefings-statements/joint-statement-president-donald-j-trump-united-states-america-chairman-kim-jong-un-democratic-peoples-republic-korea-singapore-summit/

2 https://edition.cnn.com/2018/09/26/politics/pompeo-north-korea-trip-trump-summit/index.html

3 https://www.reuters.com/article/us-northkorea-nuclear-pompeo-idUSKCN1MH02M

4 https://www.ncnk.org/node/1633

5 http://time.com/5346555/north-korea-sohae-launch-pad/

6 https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/transcript_stephen_bieugn_discussion_on_the_dprk_20190131.pdf

7 https://www.washingtonpost.com/world/national-security/us-spy-agencies-north-korea-is-working-on-new-missiles/2018/07/30/b3542696-940d-11e8-a679-b09212fb69c2_story.html?utm_term=.bab9965c819e

Huawei – US efforts ramp up as CFO's case winds its way through Canadian extradition process


Huawei CFO Meng Wanzhou is wanted in the US to face charges of bank and wire fraud and conspiracy to commit bank and wire fraud. Her arrest in Canada in December sparked an international furore of complaint and criticism. Barbara Linney and Jean-Marc Clement examine the case and Canada's extradition process.

The arrest in Vancouver, Canada on 1 December 2018 of Chinese citizen Meng Wanzhou, CFO of Huawei Technologies Co., Ltd set off a firestorm of diplomatic outrage and rampant speculation in the media and international business community regarding the reason for the US extradition request that led to the arrest.

Some questions were answered on 28 January 2019, when a superseding indictment, filed on 24 January in the US District Court for the Eastern District of New York ('EDNY'), was unsealed in part. The indictment charges Meng with bank and wire fraud and conspiracy to commit bank and wire fraud. Co-defendants Huawei and Skycom Tech Co. Ltd, a Hong Kong company that allegedly operated as Huawei's Iranian subsidiary, are charged with bank and wire fraud, conspiracy to commit bank and wire fraud and money laundering, conspiracy to defraud the United States, and conspiracy to violate and substantive violations of the International Emergency Economic Powers Act ('IEEPA'). Huawei and one of its US subsidiaries are charged with conspiracy to obstruct the ongoing grand jury investigation in the EDNY.

The IEEPA and related conspiracy charges are interesting in that they focus solely on causing unlawful export of services to Iran – both banking and financial services supplied by the 'victim' US financial institutions described but not named in the indictment and telecommunications services provided by a US citizen employee of Skycom in Iran. These are classic examples of the types of charges that are often viewed by critics of US export and sanctions enforcement policies as inappropriate extra-territorial exercise of US jurisdiction. However, the extraterritoriality argument may not assist Meng in her defence of the extradition proceedings.

The bilateral Treaty on Extradition Between the United States of America and Canada, in force since 1976, sets the rules for extradition from one country to the other of persons charged with or convicted of offences in the other country. It was originally signed in 1971 and has been subject to a few amendments over the years, notably the exchange of notes, dating back to 1974, as supplemented by two protocols agreed to between the two parties in 1988 and 2001. The treaty is implemented in Canada pursuant to the Extradition Act, which sets the procedure for the receipt and processing of extradition requests. Significantly, the act specifies that a person may be extradited even if the conduct of the accused took place outside of the requesting jurisdiction (i.e., in the case of Meng, outside of the United States).

The issue of extraterritoriality aside, the Canadian Extradition Act process is neither speedy nor summary.

Huawei CFO, Meng Wanzhou is a co-defendant in charges brought by the US Department of Justice.

Furthermore, the bank and wire fraud charges stem from alleged false statements said to have been made in the United States to US financial institutions to induce them to handle financial transactions and wire transfers prohibited by the US Iran embargo from passing through the US banking system. However, the aggregate amount of such transactions alleged in the indictment is only just slightly more than $300,000 – an amount that pales in comparison to the amounts involved in previous EDNY prosecutions of banks for IEEPA violations.

The issue of extraterritoriality aside, the Canadian Extradition Act process is neither speedy nor summary. Full due process rights, including hearings and appeals, are afforded the person whose extradition is sought. Meng currently is released on bail; her next court appearance is scheduled for 6 March. As Meng was arrested on a provisional warrant, the Extradition Act requires Canada's Minster of Justice to issue an authority to proceed if satisfied that the offence is an extraditable offence under the act. The minister is expected to make his decision prior to Meng's next court appearance. However, even if proceedings are authorised and an order of committal eventually is issued, the decision whether to order surrender is left to the minister – a decision that itself is subject to judicial review.

Not surprisingly, then, extradition

proceedings in Canada can move very slowly, but US prosecutors have a history of staying the course, as illustrated by the recent case of the owner of a Canadian telemarketing operation who, according to a September 2018 US Department of Justice press release, was extradited 'after more than 10 years of litigation in Canada' to California, where he was convicted and sentenced on fraud charges.

On the other hand, the Extradition Act prohibits the minister from ordering surrender if the extradition request is politically motivated. Political motivation is a not implausible argument in the Meng case, given President's Trump's statement that he 'would certainly intervene' in the case if he 'thinks it's good for what will be certainly the largest trade deal ever made' – a position that did nothing to calm already fractured US-China and US-Canada relations. The situation became more politically charged in late January when Canada's ambassador to China commented on the case, citing various grounds on which Meng might fight extradition. He later resigned after being criticised for giving the impression that the extradition process could be politicised.

The Extradition Act prohibits the minister from ordering surrender if the extradition request is politically motivated.

Back in the EDNY, the case is moving forward despite the slow pace of the Meng extradition proceedings in Canada. The press release issued by the EDNY's US Attorney's office when the indictment was unsealed makes clear that the investigation is ongoing and includes a statement from the Secretary of Commerce acknowledging the assistance of the Office of Export Enforcement in the investigation, as well as a plea for companies with information about additional misconduct by the indicted defendants and their related entities and principals to come forward to assist in the investigation. Involvement of OEE in this ongoing investigation can only mean that investigators are gathering information about companies involved in exports and re-exports to Huawei and Skycom – the inevitable result of which will be a considerable burden on companies who are called upon to respond to subpoenas and the financial institutions who handle their export-related financial transactions. As the investigation grows, US exporters may begin to ask themselves whether business with Huawei is worth the cost.

Barbara D. Linney is a partner and co-lead of the international trade practice team at BakerHostetler in Washington DC. Jean-Marc Clement is name partner at Clement Law Office, Montreal.

blinney@bakerlaw.com

jean-marc@clement-tradelaw.com

Huawei indictments: economic sanctions and export controls risks for US and multinational companies

China's telecom giant Huawei has long been in the sights of the US lawmakers who suspect the privately-owned company of possibly being involved in Chinese espionage activities – and sanctions violations. Recent indictments (and the arrest in Vancouver of CFO Meng Wanzhou) raises the heat for companies in the Huawei supply chain, as Timothy O'Toole, Brian Fleming, Collman Griffin and Caroline Watson explain.

Longstanding tensions between the United States government and Huawei Technologies Co., Ltd. ('Huawei'), came to a head in late January 2019, when the acting US Attorney General announced two separate indictments against the Chinese telecoms equipment giant.

In one indictment in Eastern District of New York ('EDNY'), Huawei was charged[1] with violations of the International Emergency Economic Powers Act ('IEEPA') and the Iranian Transactions and Sanctions Regulations ('ITSR'), along with related bank fraud, wire fraud, money-laundering, and obstruction-of-justice charges, both for alleged substantive and conspiracy violations. The EDNY charges arise out of Huawei's alleged scheme to surreptitiously conduct business in Iran, in part by deceiving US financial institutions and regulatory authorities. Co-defendants in the EDNY indictment include Huawei's US subsidiary Huawei Device USA, Inc. ('Huawei USA'); the Hong Kong company Skycom Tech Co., Ltd. ('Skycom'), an (alleged) Huawei subsidiary; and Huawei CFO Meng Wanzhou, along with individuals whose names have been redacted from the indictment as published.

In a second indictment in the Western District of Washington ('WDWA'), Huawei subsidiaries Huawei USA and Huawei Device Co., Ltd. were charged[2] with conspiring to steal trade secrets from T-Mobile USA, Inc. ('T-Mobile'), as well as related wire fraud and obstruction-of-justice charges. The WDWA charges arise out of Huawei's alleged attempts to steal an innovative smartphone-testing robot technology known as 'Tappy', in order to improve and develop Huawei's own robotic technology known as 'xDeviceRobot'.

Since at least 2008, the Committee on Foreign Investment in the United States ('CFIUS') has prevented or severely limited several Huawei investments in the United States – and even investments in the United States by companies doing business with Huawei. (CFIUS is an inter-agency government committee that can prevent foreign investment in the United States on national security grounds.) The US intelligence community and several prominent senators and members of the House of Representatives have warned that Huawei may use investments in the United States to gain access to critical infrastructure, such as telecommunications network routing equipment, and then eavesdrop on US domestic communications on behalf of the Chinese government.

Now, however, economic sanctions and export controls appear to be the most prominent national security risk in US authorities' minds when dealing with Huawei. Furthermore, the Huawei indictments appear to be part of a larger trend of China-focused economic sanctions and export control enforcement. Notably, in the year leading up to the Huawei indictments, the US Department of Justice ('DOJ') secured criminal convictions of numerous individuals for wilfully providing sensitive integrated circuit technologies to China; the US Department of Treasury, Office of Foreign Assets Control ('OFAC') announced its first enforcement action against a Chinese company in connection with apparent Iran sanctions violations; and the US Department of Commerce, Bureau of Industry and Security ('BIS') increased the number of Chinese and Hong Kong companies on the Entity List to more than 180, surpassed by only Russia in terms of the total number of Entity List companies.

The Huawei indictments and increased enforcement do not only

create risk for Chinese companies; US and multinational partners of Chinese companies may now face heightened enforcement risk, as well. Of course, even before the Huawei indictments, US and multinational companies faced legal risks for any conduct that US authorities might deem supportive of a Chinese partner's alleged efforts to violate US economic sanctions or export control law – as any company seeking to navigate BIS's deemed export rule or Entity List in China can attest. After the Huawei indictments, however, it seems clear US authorities are focusing even more of their attention on China, creating greater risk even for unwitting involvement in China-related conduct that the US government may deem malign.

Accordingly, we see the Huawei indictments as a useful illustration of the kinds of economic sanctions and export controls risks that US and multinational companies should consider when doing business in China or with Chinese partners. Specifically, we offer four take-aways for legal and compliance practitioners, set forth below.

1) Use the Huawei indictments to fine-tune existing compliance programmes – especially since you may now be on notice about economic sanctions and export controls risk in China.

According to the EDNY indictment, Huawei, its subsidiaries, and its CFO Meng Wanzhou allegedly lied to US financial institutions about the company's dealings with Iran and relationship with Skycom, the alleged subsidiary based in Hong Kong that was at the centre of the alleged scheme to re-export US-origin items to Iran. Similarly, according to the WDWA indictment, two Huawei subsidiaries sought to steal technology for the 'Tappy' robot from T-Mobile, the US subsidiary of the German telecommunications company Deutsche Telekom AG.

Both indictments characterise the US persons involved as victims of Huawei's alleged fraud and unfair technology acquisition strategy. Furthermore, we are not aware of any US persons who have faced enforcement actions in connection with the Huawei indictments thus far, although the case is ongoing.

However, US or multinational companies caught up in the next big China-focused enforcement action may not be so fortunate.

Witting involvement in Huawei's alleged misconduct would almost certainly give rise to significant enforcement risk. For example, as a point of comparison, in January 2018, an investigation into Chinese and Russian attempts to gain access to US controlled radiation hardened integrated circuits ('RHICs') resulted in a criminal conviction for a US citizen in Texas who helped fulfil purchase orders for foreign purchasers while certifying his company was the end-user for the products.[3]

Simple list-based screening for OFAC specially designated nationals ('SDNs') or BIS denied parties may no longer be enough.

Furthermore, even unwitting involvement in Huawei's alleged misconduct could give rise to legal risk if US authorities determine that a Huawei partner had failed to conduct reasonable due diligence. This risk is only exacerbated by the Huawei enforcement actions, which may give US authorities grounds to argue that US and multinational companies should be on notice for misconduct similar to that in which Huawei is alleged to have engaged. Specifically, US authorities may now argue that a US or multinational bank or supplier should know to take extra precautions when dealing with companies similar to Huawei, potentially resulting in civil liability if an enforcement action is later launched. Furthermore, while T-Mobile's 'Tappy' robot may not have been export-controlled at the time of the alleged attempted trade secret theft from T-Mobile, the enactment of The Export Control Reform Act of 2018 ('ECRA') will likely soon expand the list of technologies subject to US export controls, potentially creating liability in similar situations in the future.

Accordingly, we recommend that US and multinational companies take advantage of the Huawei indictments to fine-tune their economic sanctions and export control compliance programmes, in particular in connection with China. Simple list-based screening for OFAC specially designated nationals ('SDNs') or BIS denied parties may no longer be enough. Companies may need to be on the lookout for potential evasive behaviour as well, even by Chinese partners that are as well-established as Huawei. Compliance programmes should thus be able to spot and resolve 'red flags' that a Chinese partner may be engaged in misconduct similar to the alleged scheme to re-export US items to Iran at the center of the EDNY indictment. Failure to take sufficient care may empower US authorities to argue that a company knew or should have known about a potential violation of US law, increasing legal risk.

2) Consider auditing past dealings with Huawei

The two Huawei indictments cover a narrow sliver of the telecommunications giant's global business and may, potentially, implicate only a small portion of the company's economic sanctions and export control-related misconduct. Notably, in the 2016 subpoena that first indicated a serious US government investigation into Huawei's alleged export control violations, BIS reportedly requested information on Huawei's dealings in other embargoed countries such as Cuba, Iran, North Korea, Sudan, and Syria – all countries where the Chinese telecoms company is known to do business. Accordingly, in addition to the EDNY indictment announced already, Huawei may face additional enforcement actions in connection with dealings in Cuba,

North Korea, Sudan, and Syria in the future.

In addition, the WDWA indictment suggests that attempted technology theft was part of Huawei's way of doing business. In one telling detail, the indictment alleged that one Huawei Chinese subsidiary had a formal policy offering bonuses to employees who stole confidential information from competitors. If this allegation is true, Huawei may have sought to steal other technologies as well, including US export-controlled technologies, potentially giving rise to additional enforcement actions. Such actions may create risk for other US and multinational companies that have done business with the company in the past five years.

Accordingly, financial institutions may want to consider auditing their past dealings with Huawei, in particular when financing was provided in US dollars or services were provided by US persons or from the United States. Similarly, Huawei suppliers may want to consider auditing any transactions with Huawei where a US export licence was required, or where US goods, services, or technology were otherwise exported, re-exported, or transferred to the Chinese company.

The focus of these audits should be to search for red flags, perhaps unnoticed at the time, indicating that Huawei may have used US financing, goods, services, or technology in unauthorised ways, for example in support of the export or re-export of US items to Cuba, Iran, North Korea, Sudan, and Syria. If any red flags are uncovered, a company should confer with US counsel to determine the best approach to remediate the issues, which could potentially involve voluntarily self-disclosing the information to US authorities. Under the right circumstances, a voluntary self-disclosure can help frame the narrative in the company's favour and earn credit with US authorities for cooperation.

Links and notes

[1] https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial

2 https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade

3 https://www.justice.gov/usao-edtx/pr/texas-man-sentenced-conspiring-illegally-export-radiation-hardened-integrated-circuits

3) Develop contingency plans for a Huawei entity listing or denial order

Despite the DOJ's two criminal indictments against Huawei, neither the Chinese company nor any of its subsidiaries are currently on the Entity List or subject to a BIS denial order,

Huawei's current suppliers should consider contingency plans in case an entity listing or denial order occurs and all exports or re-exports of US items to the company are prohibited.

which would prevent the supply of almost all US items to the company, including entirely civilian items designated as EAR99. However, the Huawei indictments significantly increase the risk of such action.

Notably, the DOJ criminal indictment of ZTE Corporation – another Chinese telecommunications company alleged to have engaged in similar export control violations in connection with Iran – was preceded by ZTE's inclusion on the Entity List. A similar fate could await Huawei. Such a penalty would give the US government significant leverage over the Chinese telecommunications equipment provider, which could ultimately lead to a guilty plea, much in the same way it did with ZTE.

Accordingly, Huawei's current suppliers should consider contingency plans in case an entity listing or denial order occurs and all exports or re-exports of US items to the company are prohibited. For example, suppliers should consider how to mitigate any losses that may arise from contracts with Huawei that may be cancelled, legal strategies for terminating any contracts with Huawei if export restrictions are imposed while minimising potential liability, and closely monitoring the Huawei enforcement action to ensure that any shipments to the Chinese company can be stopped, if necessary.

In addition, although the time has likely passed to insert sanctions and export control compliance and termination language into ongoing contracts with Huawei, companies doing business in China can still use the Huawei indictments to revisit their current compliance language for the relevant contracts – and insist on strong contractual language in future dealings with partners that may present similar risks.

4) Assess the impact of the Huawei indictments on other US government dealings

Finally, the Huawei indictments are likely to have several follow-on effects for other dealings with the US government, which companies should fully assess before deciding whether to continue dealings with the company.

In the CFIUS context, US authorities have long taken a hard line regarding Huawei and have insisted on severing ties with the company as a condition for approval of sensitive investments in the United States. One notable example is the agreement by Germany's Deutsche Telekom AG and Japan's SoftBank Group Ltd to stop using Huawei equipment so as to obtain CFIUS approval for the merger of their two US subsidiaries, T-Mobile and Sprint Corp. In light of the Huawei indictments and the newly enacted Foreign Investment Risk Review Modernization Act of 2018 ('FIRRMA'), companies should expect CFIUS to scrutinise Huawei connections even more closely in connection with any foreign direct investment in the United States.

Similarly, in the US government contracts context, the National Defense Authorization Act for Fiscal Year 2019 now prohibits US government agencies from procuring or obtaining any equipment, systems, or services, that use Huawei components as substantial or essential components. Companies doing significant business with the US government may therefore also wish to assess their relationship with Huawei going forward.

Timothy O'Toole (member), Brian Fleming (member), Collman Griffin (associate) and Caroline Watson (associate) are attorneys at Washington, DC law firm Miller & Chevalier Chartered.

www.millerchevalier.com

Contractual protections: considerations and pitfalls in sanctions provisions

The deal is finally ready to be signed. The bubbly is flowing and the bonuses are already being spent. But has anyone considered the potential impact of sanctions on the transaction going through? Roger Matthews cautions against leaving consideration of sanctions risk to the last minute.

In commercial and corporate contract negotiations, sanctions clauses can often end up as something of an afterthought. But sanctions have the potential to cause significant disruption to commercial dealings, and inadequate attention to compliance can expose parties to a risk of enforcement action.

This article sets out some key considerations that contracting parties should consider, and some of the pitfalls that commonly occur.

Types of contract and the aim of sanctions provisions

Sanctions considerations are relevant to many contracts that have an international dimension (and to some that don't).

But different types of contract will raise very different concerns: in a transactional contract, such as a corporate contract, a purchaser will want extensive reassurance as to the past sanctions compliance history of the target; in an export contract, a seller may be anxious to know to where and to/by whom its products are going to be sold on or used; an investment fund will want reassurance that money provided by key investors is not blocked or frozen funds; a lender will want reassurance that the monies loaned are to be used in compliance with relevant sanctions. Parties and their advisers should identify up front what sanctions risks that they most need to guard against, in order to assess what provisions are needed.

Parties and their advisers should identify up front what sanctions risks that they most need to guard against, in order to assess what provisions are needed.

Sanctions provisions generally have one of two objectives – either to ensure compliance with relevant sanctions laws in the completion and performance of a contract, or to anticipate and provide for the possibility that new sanctions laws, introduced after signing the contract, might obstruct the intended performance of the contract. It is not possible to cover all variations in one article, but some common themes can be identified.

Which jurisdictions' sanctions laws are we concerned with?

At the outset, parties need to be clear which jurisdictions' sanctions they need to comply with.

The jurisdictional reach of each country's sanctions laws is different. For the EU, they will apply to persons/entities established in the jurisdiction, and to any activity done within the jurisdiction; jurisdiction can often extend to other circumstances, too. As a minimum, each party to a contract should be clear as to the jurisdiction in which it is established, and to identify the jurisdictions whose sanctions laws might apply to any aspects of the performance of the contract.

A company may have key personnel from a different jurisdiction involved in a contract, such that those personnel may need to respect that jurisdiction's laws even if the company itself does not. In such a case, the company may want either to ensure that the contract

includes that country's sanctions laws in the definition of 'sanctions' (in addition to the jurisdictions that apply directly) or that those personnel are recused from any involvement in the contract or its performance that might put them in breach.

Often parties have an internal policy that commits to wider sanctions compliance. For example a party may have a policy of always complying with US or EU sanctions for reputational reasons, even in cases where, jurisdictionally, it does not need to.

Secondary sanctions in particular should be considered here: these US measures are not binding prohibitions on the conduct of non-US persons, but many non-US businesses have a policy of avoiding sanctionable activity nonetheless.

It is common to see contract terms drafted by reference to activities prohibited by 'applicable sanctions' without clarifying whether or not that expression is intended to include conduct that is sanctionable under US secondary sanctions.

The withdrawal of the US from the JCPOA illustrates this: European companies with Iran-related contracts that provided for the possibility to exit where performance was obstructed by applicable sanctions may have found that the clause offered little assistance if the definitions did not clarify that the expression was to include US secondary sanctions.

The recent update to the EU Blocking Statute has introduced a further complication here, introducing a degree of EU sanctions risk for an EU company that gives a blanket contractual commitment to respect US secondary sanctions, although it remains to be seen whether the EU approach to enforcement of the Blocking Statute has changed in light of the renewed focus on it in 2018.

Contractual representations and warranties

Representations and warranties are a key element in offering reassurance that entering into, and performing, a contract will not expose a party to sanctions compliance risk.

Examples of representations that are commonly sought include:

- that the counterparty is not, and is not owned or controlled by, a person who is designated in a relevant jurisdiction (note that it is not only the EU and US that maintain lists of designated persons);
- that the counterparty does not operate in certain jurisdictions (e.g., Iran, Syria);
- that the counterparty has never been investigated/prosecuted for a sanctions breach;
- that the counterparty has not breached sanctions in the past five years;
- that the counterparty has in place, and applies, an effective sanctions compliance policy and effective procedures to ensure compliance.

Accompanying such representations, it is common for parties to seek and to give undertakings going forward. These might include:

- not to deal with a person who is designated (by a relevant jurisdiction) or owned or controlled by a designated person;
- not to export goods to a certain jurisdiction;
- not to use funds loaned under a loan agreement in a particular way;
- to maintain and apply an effective sanctions compliance policy and procedures.

Precisely what representations and warranties are appropriate will depend on the nature of the contract, and a range of other factors.

This is by no means an exhaustive list.

In identifying what representations and warranties are necessary, a party should consider what concerns it has. For example, in a one-off purchase transaction, a party may not mind that the counterparty has a poor sanctions compliance history provided it is satisfied that this transaction is compliant, whereas a bank offering services to a client very likely will. Lenders will likely want reassurance that their loan is not loaned for a sanctions-breaching purpose, and that money used to make repayments is not derived from any sanctions-breaching activity.

Separately from ensuring compliance with existing sanctions, parties should consider the possibility of new, perhaps unanticipated sanctions.

Which sanctions lists?

A common source of ambiguity in representations and warranties arises from references to 'listed persons', 'designated persons' or other such expressions. Parties should be clear how wide is the commitment (or representation) that they are seeking or giving. In the US, both OFAC and BIS maintain a number of sanctions-related lists with the implications of a listing varying considerably.

For example, is a warranty not to deal with 'designated persons' intended to include an SSI Directive 3 listed entity? The EU currently only

Force majeure and sanctions clauses

Separately from ensuring compliance with existing sanctions, parties should consider the possibility of new, perhaps unanticipated sanctions. New designations in a country already subject to restrictions are easier to anticipate; fresh sanctions consequent on a future event rather less so. What constitutes an event of *force majeure* is, under English law, a matter for negotiation between the parties (unlike many civil law systems). The wider the *force majeure* clause, and the more clear that the parties intended that a sanctions development is an event of *force majeure*, the more likely it is that it will be held to be.

However, where parties have identified potential sanctions issues as a risk in advance, the preferred approach is often to have a dedicated sanctions clause where the nature of potential sanctions risk, and its likely consequences for the contract, are more clearly addressed. In particular, such a clause might clarify whether the occurrence of such an event terminates the contract or merely suspends it, and where any liabilities lie, and may clarify the often ambiguous position where performance is not entirely blocked by sanctions, but is rendered substantially more expensive.

has two main lists (the Asset Freeze list and the Investment Ban list –the latter relating to the Russia sanctions), but it has operated other lists in the past (for example, in the case of Burma/Myanmar) and may do in the future. It is common to see an undertaking including a commitment not to deal with parties on 'the EU consolidated list' when the parties may not have intended to include the Investment Ban list entities in the undertaking.

Export and sanctions licences

Where a contract envisages the movement of controlled goods or technology or services related to them, or any trade with countries targeted by sanctions, the parties should consider the potential need for sanctions or export licences. The contract might include commitments by the acquiring party to verify end use and end-users of the goods in question, and should attribute clearly both who has the obligation to obtain any necessary licences, and what are the consequences in the event that a licence is either refused, or significantly delayed. A failure to address in advance the implications of difficulties in obtaining licences risks ending up in dispute further on. Where products originate in the US, or contain components that do, it may be necessary to obtain a US export licence for the re-export between other countries.

Merely including a generic sanctions clause is unlikely to offer much protection.

Brexit

With Brexit seemingly on the horizon, and with many contracts being governed by English law, it is prudent to ensure that contracts provide for the need to comply with UK sanctions laws as well as (or in place of) EU sanctions laws in the definition of 'sanctions laws'. Many existing contracts do not do that, having been drafted pre-2016 on the assumption of UK being an EU Member State. With UK sanctions likely to stay substantively very close to EU sanctions for the foreseeable future, the risk here may be limited for the immediate future, but will become more acute as UK sanctions gradually diverge from EU sanctions.

Be prepared; be very prepared

With sanctions remaining a popular tool for western (and other) governments, and with the nature of sanctions restrictions becoming increasingly diverse, it is ever more important that parties negotiating international contracts of all sorts identify up front the sanctions risk they might be exposed to and ensure that these are properly addressed. Merely including a generic sanctions clause is unlikely to offer much protection.

Roger Matthews is a partner in the International Trade and Regulatory practice group at Dentons in London.

Roger.Matthews@dentons.com

Leading practices for export compliance audits



Getting the nuts and bolts of a compliance audit right can be an invaluable step to wider business successes, write Amie Ahanchian, Brandon Barela and Sarah Blank.

Developing a robust audit programme can be a game-changer for corporations navigating the increasingly complex world of global trade, as an effective audit programme is clearly an integral element of any world-class export compliance programme. In this article, we set forth leading practices for executing an export compliance risk audit and explain why audits are a necessary aspect of a company's internal control framework and overall compliance life-cycle.

Compliance audits vary in type – from organisational self-assessments, corporate-level export compliance reviews, internal audits, external assessments, and government-directed audits. The scope of each audit can also vary significantly – from general regulatory assessments policy compliance, transaction-level reviews, and so forth. A well-executed audit involves planning, performing, reporting and implementing improvements based on the results. In this article, we set forth a blueprint for conducting an internal audit of a company's export compliance activity.

Thinking ahead to the results of the audit

While it is important for companies to conduct audits to evaluate regulatory compliance, assess the effectiveness of existing corporate objectives and processes, and identify and analyse risks, what is equally as important is how export compliance leaders incorporate the audit findings into their organisation's compliance life cycle. To be impactful, compliance leaders should use findings to further vet the root cause(s) of compliance errors, formulate and execute a plan for corrective action(s), and leverage the outcome of these analyses as the basis of future compliance training programmes. In other words, the audit should not be a unique event, but rather a periodic (e.g., quarterly) practice that is implemented within the organisation's trade compliance framework.

The audit should not be a unique event, but rather a periodic practice that is implemented within the organisation's trade compliance framework.

Although maintaining a strong internal control framework is the foundation of an export compliance programme, export compliance departments are often 'lean' – and corporate leadership may not recognise the true complexity of complying with the regulations. In addition to identifying risks, an audit programme can positively shine a light on these challenges by demonstrating what an organisation is doing well and where improvements can be made. An audit may even result in every export compliance professional's dream – getting the resources, staffing and technology tools needed to develop an exceptional export compliance programme.

For these reasons, as an organisation begins to plan the audit, it should consider how the findings will be used within the trade compliance framework and with respect to the business overall.

Planning the audit

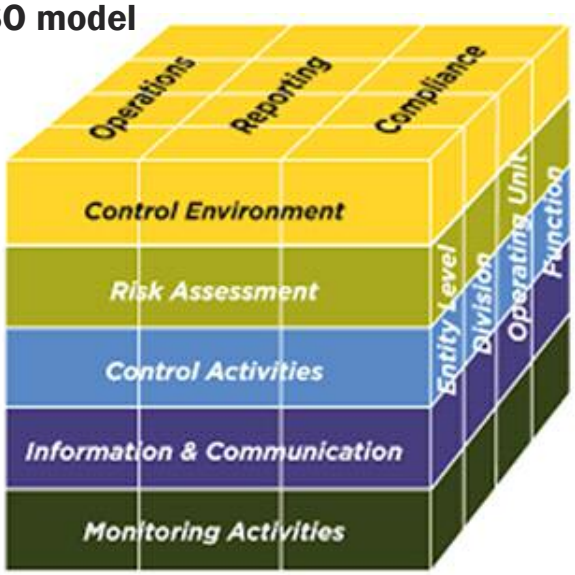
In planning the audit, the core team should define the objectives, outline the scope, identify the steps to be taken and reserve the required resources. The high-level scope and objectives should be established at the outset which will then later be refined upon completion of the risk assessment.

Complete a risk assessment

In approaching an audit, the organisation should conduct a risk assessment which identifies the highest areas of risk to the business.

Looking to the Committee of Sponsoring Organizations of the Treadway Commission ('COSO') – which defines itself as 'dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence' – risk assessments are one of the five components comprising an effective internal control system for any company. Other

The COSO model



components are (i) the control environment, (ii) control activities, (iii) information and communication, and (iv) monitoring activities. Please refer to the depiction of the COSO model (see illustration 'The COSO Model') , which has been adopted as the generally accepted framework for internal control and is widely recognised as the definitive standard against which organisations measure the effectiveness of their systems of internal control.[1]

Conducting an objective risk assessment is a valuable way to target areas for closer review as it will help focus time and resources on priority areas with the most risk. The risk assessment consists of developing a risk matrix that compares the likelihood of the event or activity against the possible impact. The likelihood criteria should consider factors such as volume/frequency of activity, existence of policies and processes, employee training in a given area, recent violations or voluntary disclosures, and newly implemented corrective actions. Assessing the potential impact requires a consideration of the possible results stemming from a compliance gap in the area. This can range from something relatively minor, such as a shipping delay, and can increase in severity to include fines and penalties levied on the organisation or complete denial of export privileges.

Specific topics included in the risk assessment will vary from one organisation to another, but some key areas for assessment that pertain to most exporting organisations include looking at jurisdiction classification determinations, technical data/ technology transfers, foreign-person employees, licences and authorisations, recordkeeping, restricted-party screening, international travel and visitor access. For those companies with items subject to the International Traffic in Arms Regulations ('ITAR'), other areas could include Part 130[2] reporting, Part 129[3] brokering and so forth. It is also helpful to review recent enforcement trends to identify topical areas of concern to the US government and to assess whether the organisation has any risks in those areas.

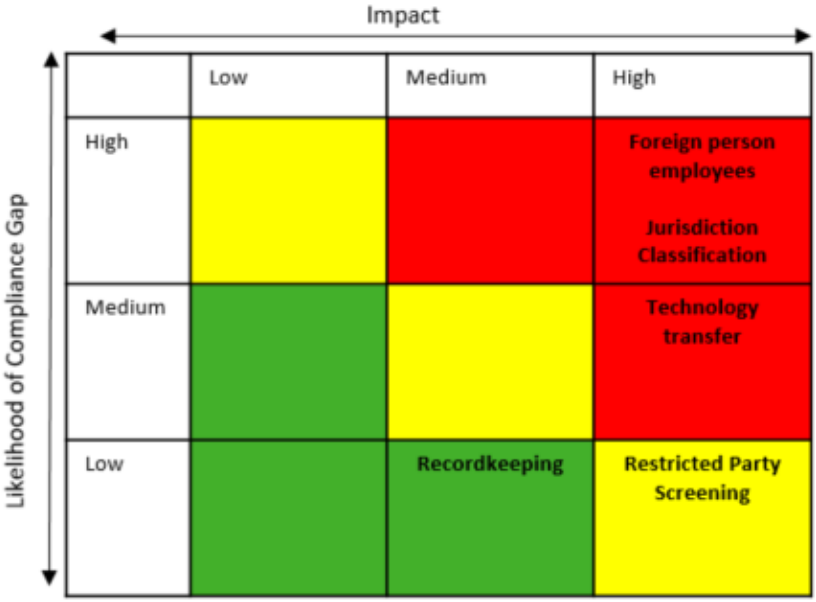
In the figure below, a fictional company has weighed possible compliance gaps for their organisation. In this example, the organisation does not have a robust jurisdiction-classification process or internal controls for foreign employees. Therefore, the likelihood of having a violation is high, as is the impact of a possible violation. In contrast, the organisation has a strong restricted-party screening process. As such, the likelihood of having a restricted-party screening violation is low, but the impact of a violation would be high.

The risk assessment can also be a valuable communication tool to gain management support for the time and resources that will need to be allocated for the audit. By clearly articulating the applicable risk(s) within the organisation, the trade compliance manager can bolster their case for conducting the review.

Refining the scope and objectives

Once a risk assessment has been conducted to identify the highest areas of risk throughout the organisation, the scope of the audit can be refined. Although this sounds like a simple step, it is important to agree upon the intent of the audit. This can range from conducting a high-level health check on a very narrowly focused matter,

Weighing up compliance gaps



such as compliance with temporary hardware licences, or can entail a full-scale audit to validate compliance with all regulatory and organisational recordkeeping requirements. The audit management team also needs to determine if the review will be conducted company-wide or be focused on a specific division, location or product line. Conducting a risk assessment up front will help the team determine the appropriate audit scope to mitigate targeted risks and meet the overall objectives.

An additional aspect to consider is who will be conducting the review. There are certain areas where a self-assessment conducted by the local trade compliance group is appropriate. In other circumstances, it may be better for a corporate-level compliance group to be involved. There are also scenarios where engaging an external auditor may be the most objective way to identify compliance gaps, and in some cases involving US government penalties, the use of an external auditor is directed by the US government. Companies who have undergone consent agreements with the US Department of State Directorate of Defense Trade Controls often undergo multiple corporate-wide audits with some conducted by an external provider and other smaller reviews conducted internally.

External auditors are valuable in a number of ways. They can provide an objective perspective and provide insights into industry-leading practices. They can also provide additional resources for a larger-scale review, such as those required under consent agreements or government-directed audits. In the case where the headquarters or corporate office is reviewing business operations in multiple jurisdictions, it may be worthwhile to engage with a local auditor that understands the nuances of the local regulations and can speak the local language.

The purpose and scope of the review should be clearly communicated to the management of the organisation being reviewed to set expectations of what will be reviewed, including the resources and time commitments required. The scope, objectives and methodology of the review should be documented in an audit plan.

Conducting the review

Any review should include a combination of document review (policies, procedures and desktop instructions), employee interviews (including over-the-shoulder reviews), and transactional testing. Reviewing existing policies, procedures, and desktop instructions is needed to design the testing and develop interview questions. The review should confirm that the local guidance documents are aligned with both corporate policy and local regulatory requirements.

In multiple jurisdictions, it may be worthwhile to engage with a local auditor that understands the nuances of the local regulations and can speak the local language.

In conducting employee interviews, the auditor should gauge the employees' understanding of the existing policies and procedures and whether or not the day-to-day activity is being conducted accordingly. As technology becomes increasingly important in export compliance, another valuable exercise beyond soliciting verbal explanations is having the employee show the auditor how they use the automated tools to conduct transactions (e.g., walking the reviewer through their process in conducting a restricted-party screening).

Depending on the scope of the review, the auditor should endeavour to speak with a wide variety of employees, including those outside of trade compliance, such as shipping/logistics, procurement, information technology ('IT'), security and/or engineering. For organisations that have network restrictions in place to limit access to export-controlled data, the auditor should do an over-the-shoulder review with IT under various profiles to understand how these network limitations are put in place.

For transactional testing, auditors should select a sampling of transactions to review that is representative of the organisation's trade profile. The sampling should include a broad range of criteria based on the volume and type of transactions involved.

For example, to conduct a review of hardware shipments, the auditor should select a mix of samples, including shipments authorised under varying government authorisations (or exceptions), and a diverse array of products, associated export classifications, export destinations, end-users, freight-forwarders and so forth. The testing should involve looking at the actual export declaration against the licence or authorisation, shipping paperwork and internal files/data to validate compliance with the regulations and relevant procedures.

Other types of testing involve reviewing licence reports, confirming restricted-party screening was conducted for all relevant transactions, testing the jurisdiction and classification determination, or reviewing visitor-access files and technology control plans. Another important area to review is training records and an assessment of whether the training was sufficient.

Reporting

As important as conducting the review itself is documenting the audit results. The level of documentation varies again based on the scope of the review and may be as simple as a few PowerPoint slides and as complex as a detailed report and testing logs.

It is important to refer back to the audit plan to verify that objectives have been met.

The report should include documentation of areas reviewed, deficiencies observed and recommendations for improvement.

After the audit

There are a number of different steps for the organisation to take after an audit. Typically, the audit will include a management response or development of a compliance-improvement plan. Before committing

to corrective actions, the organisation may wish to conduct root-cause analysis to better understand the deficiencies and, as such, design better solutions. For errors identified in transactional testing, additional analysis should be done to assess whether the errors were clerical or systemic in nature.

Common examples of actions to be taken following a review include:

- Providing employees with additional training;
- Modifying or implementing new policies and procedures;
- Identifying and implementing new technology solutions; and
- Hiring additional team members or better distributing responsibilities throughout the organisation.

Links and notes

[1] https://www.coso.org/Pages/aboutus.aspx.

[2] https://info.knowledgeleader.com/bid/161685/what-are-the-five-components-of-the-coso-framework.

[3] 22 CFR Part 130.

[4] 22 CFR Part 129.

If the audit identifies a regulatory violation, the organisation also must determine if they want to submit a voluntary disclosure to the relevant government agency.

Corrective actions from the audit should be actionable and measurable. Follow-up is important to ensure that corrective actions are appropriately implemented. Audits may fail to achieve their purpose if corrective actions are not implemented or are only partially or incorrectly implemented.

Conclusion

In summary, a successful audit involves planning, performing, reporting and implementing improvements based on the results. Developing a risk assessment will help the audit team focus on key areas to review, and selecting the right team to perform the review at the right level will aid in gaining valuable insights about the overall health of the export compliance programme. Clearly, export compliance programmes should be dynamic, and on-going audits are a valuable tool to identify areas for improvement. Companies should keep in mind that an audit may result in additional training, modification of policies and procedures, identification of technology solutions, or providing justification for additional export compliance staff – all important aspects of the trade compliance life-cycle. Most notably, audits should be embraced as a tool to make improvements in an export compliance programme.

This article represents the views of the authors only and does not necessarily represent the views or professional advice of KPMG LLP.

Amie Ahanchian is a managing director, Brandon Barela is a manager and Sarah Blank is a senior associate in the Trade & Customs Services practice of KPMG LLP.

aahanchian@kpmg.com
bbarela@kpmg.com
sblank@kpmg.com

Who pays the ferryman?

WorldECR explores the sanctions screening solution developed by the other Kharon, brainchild of a small pantheon of former US Treasury experts.

In Greek mythology, Kharon is the ferryman who transports the souls of the newly dead across the river Styx to Hades. The river Styx was a treacherous and difficult channel to cross, and famously it was only Kharon who was entrusted to undertake this unenviable exercise. With his unique ability to navigate the ever-changing and treacherous Styx, Kharon was the only one who knew how to navigate those waters.

In the world of financial crime compliance, Kharon is a data analytics and research firm, with offerings including a web-based solution, which, it says, can help financial institutions and global corporates better understand the sanctions-related risks presented by actual and potential business partners.

Both Kharons demand a fee for their labours, but beyond that there are not insignificant differences. For Kharon the ferryman, an inflation-proof flat rate (a single obolous) was all that was required to make the journey. Kharon, the Santa Monica-HQ'd solutions provider, charges depending on solution and number of users.

Joshua Shrager (senior vice president), who took the time to describe the Kharon solution to *WorldECR*, is very much more personable than one might imagine the company's namesake being.

The solution works by identifying and mapping material connections between sanctioned entities and non-sanctioned entities.

'At our core,' says Shrager, 'we are a research and data analytics firm providing financial services and multinationals with the most comprehensive resource on sanctions-related risk. We live and breathe sanctions. We know that there are a lot of firms that provide screening software, surface adverse media and conduct due diligence work. Those services are undoubtedly important, but we are the only company laser-focused on sanctions-related risk.'

The solution works, he says, by identifying and mapping material connections between sanctioned entities and non-sanctioned entities – a task undertaken by some 30+ analysts working out of the company's California, Washington DC, New York and, imminently, London offices.

This research is empowered by a proprietary technology platform that makes easily visible ownership networks and links to sanctioned individuals and entities.

'Kharon is an augmented analysis platform. We take the world's foremost experts and couple them with the technology platform that allows them to efficiently capture and communicate research and analysis at scale. That's where we believe the power is.'

Where Kharon also excels, says Shrager, is by going beyond the 50% ownership rule threshold so many risk managers and attorneys are rightfully

mindful of. 'We don't stop at 50%. Our research will take us down to 40, 30, 20 or one percent – or even unknown ownership.' Kharon, he points out, 'is not there to make a judgement on behalf of the company as to whether it should do business with a person based on these percentages, but it identifies the potential legal and risk issues, and the relationships that are risk-relevant, and of which you would at least want to be aware.'

Global connections

A walkthrough of Kharon's 'Clearview' tool makes all apparent. Entering the name of a US entity, we find that (as we would expect) while the entity itself is not designated, the tool reveals a 'corridor' – a connection to a sanctioned entity thus: the company has a vendor-relationship with a Chinese company (Chinese company A) in the form of an arrangement by which the company sells the US company's products. Chinese company A is, again, not sanctioned. However, more than 99% of Chinese company A is owned by Chinese company B, which has been designated by the US government.

'Does this mean that a bank should be wary of having any kind of relationship with the US entity? Not necessarily,' says Shrager. 'But on the other hand, it would help formulate the questions to ask during the know-your-customer process. If, for example, the US company flatly denied having any business in China or was wary or uncooperative, that might throw up a red flag; whereas if it was candid about its business relationships, that actually might be more reassuring.'

For Kharon's 'Dynamic Analytics' offerings, which integrates Kharon's data into a client's existing screening filters or software, a client questionnaire helps set the parameters for the tool, because, as he points out, 'More data isn't always best – having the right data is more consequential. For example, two months ago a financial institution may only have wanted data on Venezuela-related 50% or more ownership risk; today they want to understand all Venezuela ownership connections regardless of percentage.'

'More data isn't always best – having the right data is more consequential.'

A bank in Florida (for example) may have greater concerns about Kingpin Act risk than breaches of the North Korea sanctions, while not all circumstances demand that a user drill down to understand 20% ownership 'risk'.

Shrager says that Kharon doesn't see itself as being in the business of making recommendations as to whether its clients should transact with a party depending on the results of a search: 'We'll bring you the statistics, the sources, the network. But at the end of the day, for a given institution, there are too many internal factors, going into the decision-making process. Each institution has its own threshold for risk. But what Kharon does is allow them to see the bigger picture and make informed choices as to whether to refrain from transactions, or conversely, use it as a business enabler.'

Behind the screens

For a sanctions-focused tool, the credentials of those behind Kharon are pretty much impeccable. CEO and chair Matthew Epstein has served both within OFAC and the Office of Terrorism and Financial Intelligence and has worked in the private sector. Collectively, the other members of the company's C-suite present similar backgrounds.

'I think one of the important components that sets Kharon apart,' says Shrager, 'is that our leadership team is bringing to bear the tradecraft we pioneered at the Treasury, we know how to train our analysts and we are tailoring our products to how we understand industry need.'

As at writing time, Kharon is set to open a London office and is looking for analysts to join its many-tongued team. 'Currently,' he says, 'we screen against the US, EU, UK, and UN lists – but that's set to grow,' (in step with the ever-growing need for such services).

Summing up, one might describe Kharon as a mythological demigod with the melancholic burden of ferrying souls to a gloomy netherworld... Or... an intuitive tool with pedigree, capable of complementing other screening tools, solutions and sanctions advice used by banks and other institutions navigating the sanctions terrain.

See: www.kharon.com

WorldECR

The journal of export controls and sanctions

Contributors in this issue

Fabian A. Jahn, rechtsanwalt, and Aleksi Pursianen, SolidPlan
www.der-rechtsanwalt.eu and https://solidplan.fi/

Shea Cotton, James Martin Center for Nonproliferation Studies
www.middlebury.edu/institute/

Barbara D. Linney, BakerHostetler, and Jean-Marc Clement, Clement Law Office
www.bakerlaw.com / www.clement-tradelaw.com

Timothy O'Toole, Brian Fleming, Collman Griffin and Caroline Watson, Miller & Chevalier Chartered
www.millerchevalier.com

Roger Matthews, Dentons
www.dentons.com

Amie Ahanchian, Brandon Barela and Sarah Blank, KPMG LLP
www.kpmg.com

General enquiries, advertising enquiries, press releases, subscriptions: info@worldecr.com

Contact the editor, Tom Blass: tnb@worldecr.com tel +44 (0)7930405003

Contact the publisher, Mark Cusick: mark.cusick@worldecr.com tel: +44 (0)7702289830

WorldECR is published by D.C. Houghton Ltd.

ISSN 2046-4797. Refer to this issue as: WorldECR [0077]

Correspondence address: D.C. Houghton Ltd, Suite 17271, 20-22 Wenlock Road, London N1 7GU, England

D.C. Houghton Ltd is registered in England and Wales (registered number 7490482) with its registered office at 20-22 Wenlock Road, London, UK

ISSUE 77. MARCH 2019
www.WorldECR.com