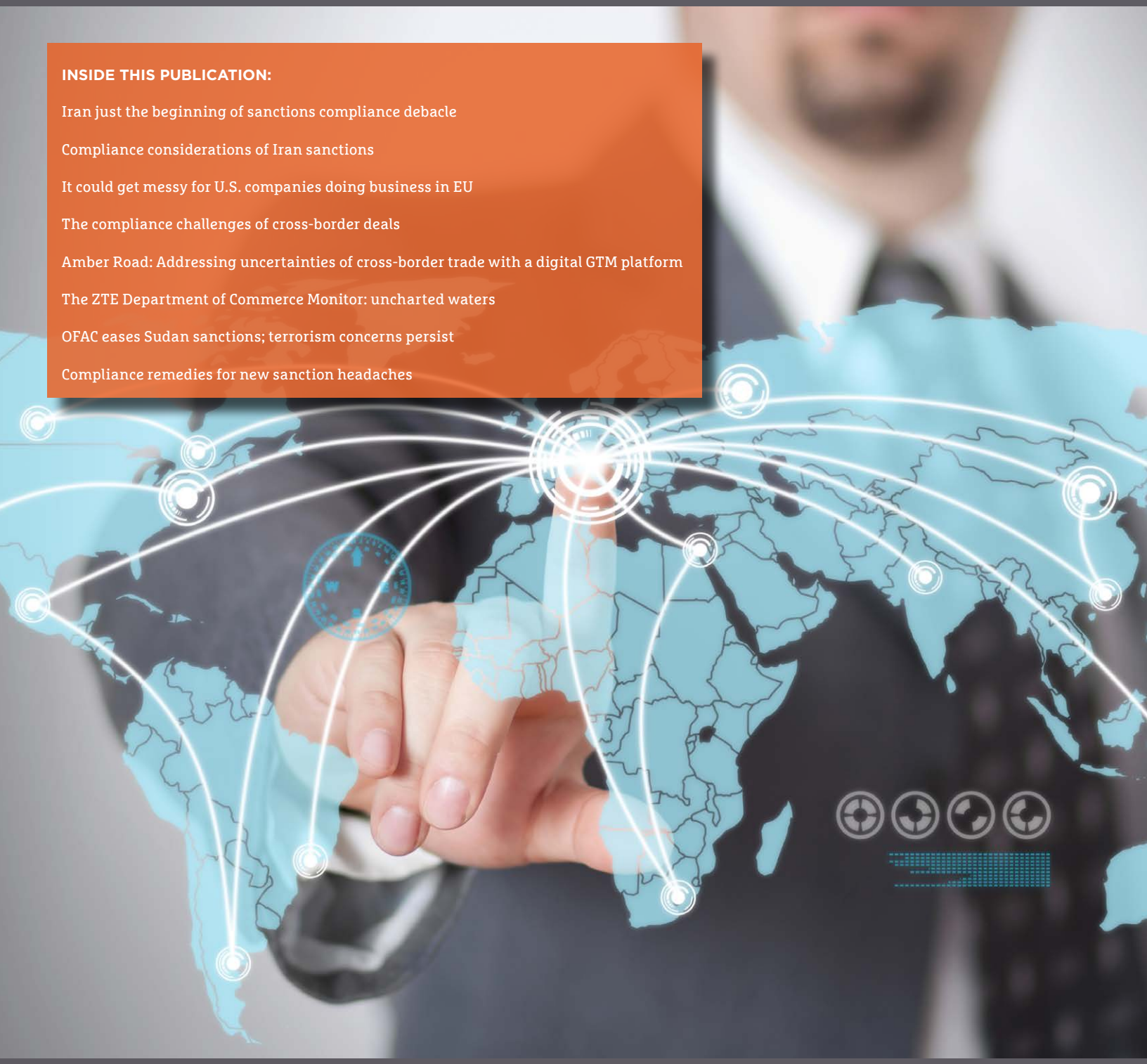
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Navigating the Worldwide Web of Trade Sanctions Laws

An e-Book publication sponsored by Amber Road POWERING GLOBAL TRADE®

About us

COMPLIANCE WEEK

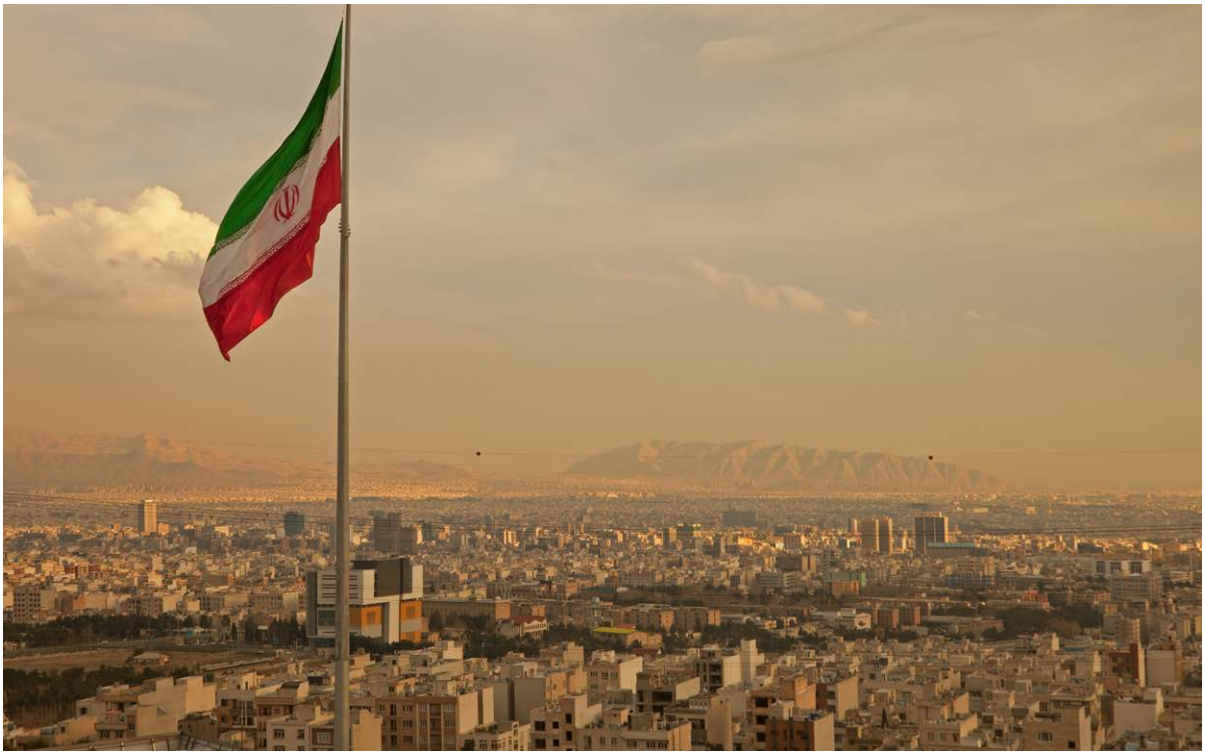
Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

Amber Road
POWERING GLOBAL TRADE®

Amber Road (NYSE: AMBR) has the largest functional footprint in the GTM software industry. Our mission is to dramatically transform the way companies conduct global trade. As a leading provider of cloud-based global trade management (GTM) software, trade content and training, we help companies all over the world create value in their global supply chain by improving margins, achieving greater agility and lowering risk. We do this by creating a digital model of the global supply chain that enables collaboration between buyers, sellers and logistics companies. Unlike other providers, we believe the digital global supply chain puzzle should be managed via a single platform that handles all aspects of global trade. Our solution provides capabilities that start with product design and continue through final order fulfillment. We replace manual and outdated processes with comprehensive automation for global trade activities, including sourcing, supplier management, production tracking, transportation management, supply chain visibility, import and export compliance, and duty management. These capabilities are not just broad, but also very deep. The strategy is to automate where possible, and make collaboration intuitive. Please visit www.AmberRoad.com.

Inside this e-Book



Iran just the beginning of sanctions compliance debacle

European companies are winding down investments in Iran, as the European Union advises them to hang in there while it looks for ways around U.S.-imposed sanctions. **Paul Hodgson** has more.

Following the U.S. decision to pull out of the Iran nuclear deal known as the Joint Comprehensive Plan of Action (JCPOA) and to re-impose sanctions, EU companies, such as carmaker Peugeot, engineering firm Siemens, and oil producers Total and BP, have begun to wind down investments and joint ventures in Iran despite the fact that European leaders have said that they will remain in the deal and find ways around the sanctions. While this is leading to confusion and uncertainty for compliance officers, both Pekka Dare, a director with International Compliance Training (ICT), and Foundation of Defense for Democracies senior advisor Richard Goldberg agreed that trying to comply with sanctions over Iran was already a compliance nightmare.

"Over the last few years, even with the JCPOA, there has still not been a stampede of European companies getting into Iran," said Dare. "You have three basic categories of banks in Europe—you have banks with U.S. DPAs (deferred prosecution agreements) such as the HSBCs and Standard Chartereds of this world; the terms of those agreements with the American authorities would preclude them from do-

ing much of anything in Iran. Then, you have banks that don't have a DPA but have a significant presence in the U.S., for example Barclays; and then a third category with very little direct exposure to the U.S. What we've seen is that all three categories are very wary of doing any direct business with Iran."

"A couple-of-hundred-billion-dollar economy in Iran is in no way worth the risk of losing a multitrillion-dollar economy in the U.S.," said Goldberg. "This means that most banks are walking away from Iran unless they are illicit, borderline financial institutions."

"Part of this has been about the uncertainty," continued Dare "and it's also been about direct and indirect exposure and the fear of secondary sanctions from the U.S. Obviously, those banks that follow UN [United Nations], EU, and OFAC [Office of Foreign Assets Control] sanctions, there will be a list of countries and, in the case of Crimea, territories where they will not do any direct business, like Syria, Iran, and Iraq. They will have policies that preclude any direct business with those countries, which means that they could not deal with a customer who has residence in that country or facilitate goods flowing directly into that country or money coming from that country."

But, with the JCPOA, said Dare, banks' customers have wanted to explore opportunities in Iran, so the challenge for banks has been to conduct proper sanctions risk assessment of their customers. "So, for example," explained Dare, "when a relationship manager onboards a commercial client in a commercial bank, part of the job is to assess the jurisdiction of that customer, who are their customers, who are they selling to. The banks have all had to work out what their tolerance is for indirect exposure. That might be where you have a customer who was wasn't necessarily selling goods directly to Iran or Syria, but might be selling those goods to hundreds of distributors, and maybe one or two of those distributors might then sell those products into a sanctioned country." Banks are struggling with this kind of indirect exposures and are wary of being involved in facilitating the flow of goods into a sanctioned country and then facing some sort of secondary sanction from the U.S.

"They're doing a lot of work on due diligence, and their risk appetite is really low. And with the Americans backing right out of the JCPOA and threatening sanctions against anybody who dares to disagree with them, that appetite is really reduced," said Dare. "A lot of banks might use an informal rule of thumb and say we would tolerate a client who had maybe 10 percent of their overall business indirectly exposed to a sanctioned country. But, we must not directly facilitate any of that business. Now all the banks will be looking again at those levels of tolerance."

Dare reiterated that the latest withdrawal from the JCPOA has not had a massive impact, because most of the banks have already made this judgment. "Even if legally under the JCPOA our clients can do business in Iran," said Dare, "what are the risks in that, and how are we going to do customer due diligence and understand the structures of entities we are dealing with in Iran? Because, while many of the sanctions were lifted, there were still many sanctions in relation to, for example, the Iranian Revolutionary Guard. So, if you are going into a joint venture with a customer who is a corporate entity in Iran, how easily could you see through the transparency of the ownership structure? There is nervousness about that."

FDD's Goldberg described the complicated situation: "From a compliance perspective, the baseline was that it was already hell to do business in Iran. Iran does not allow an independent compliance mechanism that would allow due diligence over your investments or contracts. You have to use an Islamic Republic sanctioned compliance team in the country. If you want to do a deal with an Iranian company," he said, "you have to do the due diligence that would ensure that the IRGC [Islamic Revolutionary Guard Corps] is not behind that company, but the only way to do that is to ask the Iran-based compliance team to undertake that for you. That's been a major hindrance to investment in Iran."

Goldberg added: "Now you have layers and layers of sanctions coming back. Even if you paid a whole team of compliance officers around the clock they would still be likely to fail."

Goldberg also noted that Iran could not reap the rewards of the sanctions relief because of the risk of the Iranian financial system and the fact that the IRGC was still designated as a terrorist organisation.

"There is also nervousness about the risk of litigation," said Dare. The U.S. Anti-Terrorism Act allows individuals to sue anyone who provides material support to a foreign terrorist organization, such as in the cases of *Freeman v. HSBC* and *Weiss*

v. NatWest, Dare noted. Banks have been prosecuted on a civil basis, because they've had exposure to Iran. "Even with Trump's actions it has probably not resulted in a great deal of change; it's just reinforced the banks' current policies, which are already centered around all the uncertainties," he said.

The difficulties of doing deals in Iran and still complying with sanctions law, said Goldberg, is disconnected from what European leaders are saying. "The political leadership is saying: Stay in the deal; we are going to provide ways for you to be protected from U.S. sanctions. We will bring in blocking regulations, which will shield you from any U.S. sanctions and, if the U.S. tries to fine you, you can sue in European court to try get your money back. But this is total market access being threatened; it's not just a fine."

Goldberg said the EU was considering a plan that would allow them to evade U.S. sanctions and continue to do business with Iran. Basically, Germany would allow anyone who wants to continue to do business with Iran to send the central bank—either the European Central Bank or the Bundesbank—their transactions; conversions would occur there, with all transactions settled at once. Then, a billion-dollar payment that is a total of all the European payments owed would be sent to the Central Bank of Iran. Goldberg said that it would be very difficult for U.S. regulators to parse out every transaction. "If the Royal Bank of Scotland sends a series of different messages to the central bank in Germany, which they do all the time, they will not be able to parse out which one is for Iran and which one is for Germany. The game of chicken is that the Bundesbank is daring the United States to designate a central European bank and to impose sanctions on them."

But he also said that the sanctions regime allows the U.S. to pursue individuals such as the bank's governors, its directors, or even just employees. "There are ways for the U.S. to exert an enormous amount of pressure short of designating a central bank." Goldberg added that the Iranian financial sector as a whole has been designated as being a jurisdiction of money laundering concern and that this has stayed in place throughout the life of the JCPOA.

And that's just the problems with Iran. Dare said the situation with Russian sanctions can be even more complicated. "Russia is different, because you have you have SSIs [sectoral sanctions identifiers]," he said. "There's not a comprehensive ban on doing business with Russia, but there are targeted sectoral sanctions—so the challenge there is what can happen with those sanctions regimes, because they're incredibly complicated. For example, you have a comprehensive ban on dealing with anyone in the Crimean Peninsula—but that's not simple, because how do you screen for a part of a country? You have to screen the names of ports, names of towns. ... And, of course, in eastern Ukraine many people consider themselves to be Russian and describe themselves as living in part of Russia, so there's real challenges with that. If you're dealing with a Russian bank for example, like Sberbank, you can deal with them, but you can't give them certain financial products like long-term capital loans."

Dare said this meant that compliance officers had to conduct incredibly complicated screening of any transactions involving these Russian sectors, like deep sea oil, to make sure that they're complying with sectoral sanctions. "An additional challenge for banks at the moment, with Americans daily bringing in new sanctions targeted against Russian individuals, is keeping their systems and policies up-to-date. The sheer pace and volume of change is a big challenge for banks, and all of us."

Sanctions compliance has become, in the last few years, a recognized, defined professional discipline within banks, and people with those skills are very sought after. "It's a very gray area," said Dare. "People think it's simple; if somebody or some entity is on the sanctions list you can't deal with them. But what the banks are wrestling with are these gray issues around direct and indirect exposure, and sectoral lists. There's a huge amount of fear factor around the size of the penalties as well."

Dare pointed to the new U.K. Office of Financial Sanctions Implementation (OFSI), which has new regulatory powers that allows it to connect with the National Crime Agency. "They are actively reviewing many enforcement actions at the moment. You're going to see more enforcement action in the U.K. as a result of this," he said.

"There's a lot going on," said Dare. "Banks are constantly upgrading and downgrading their risk tolerance regarding certain countries. Who knows where we are going to be with Russia in six months' time? And you've got North Korea on top of that." ■

Compliance considerations of Iran sanctions

President Trump's recent decision to withdraw the U.S. from the Iran nuclear deal will not only have severe sanctions implications for foreign subsidiaries of U.S. parent companies, but will also negatively impact EU firms. **Jaclyn Jaeger** explores.

Compliance sanctions headaches have only just begun for foreign subsidiaries of U.S. parent companies, following President Donald Trump's recent decision to withdraw the United States from the Iran nuclear deal, even as the European Union took contrary actions of its own.

In 2015, Iran committed to various limitations on its nuclear program as part of an agreement with other countries and coalitions—including the United States, the European Union, and the United Nations. This accord was called the Joint Comprehensive Plan of Action (JCPOA).

As part of the JCPOA, the United States in January 2016 lifted or waived certain "secondary sanctions," effectively allowing non-U.S. entities access to the Iranian market without risking their access to the U.S. market to pursue Iranian deals. But those sanctions were re-imposed on May 8, 2018, when President Trump issued a Presidential Memorandum ceasing U.S. participation in the JCPOA, subject to certain wind-down periods.

As described in a series of frequently asked questions (FAQs) issued by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the re-imposed U.S. sanctions will take effect following a wind-down period of 90 days (by Aug. 6) for certain sanctions, and 180 days (by Nov. 4) for others, to give time for Iran-related transactions and contracts to be completed or terminated.

Greta Lichtenbaum, an international trade partner with law firm O'Melveny, says U.S. withdrawal from the JCPOA will have "a significant impact on multinational firms that have business interests in both the United States and Iran."

Because U.S. "primary sanctions" remain in force, restricting persons and entities under U.S. jurisdiction from generally doing business with Iran, sanctions compliance implications resulting from U.S. withdrawal from the JCPOA most significantly apply to non-U.S. subsidiaries of U.S. parent companies. "For foreign companies, secondary sanctions have returned as a real threat, if they have any significant business in the United States," says Theodore Kassinger, a partner at O'Melveny.

Specifically, General License H, which authorized foreign entities of U.S. companies to do certain business in Iran, will be revoked by November. Additionally, sanctions against individuals and entities previously removed from the U.S. "Specially Designated Nationals List" also will be re-imposed.

The extractives industry, automotive and rail sectors, the shipping and shipbuilding sectors, and the financial and insurance industries will take a hard hit—but perhaps none harder than suppliers of commercial passenger aircraft and related parts and services, which had been specially licensed under the Iran nuclear deal. In an April 25 earnings call, Boeing CEO Dennis Muilenburg stressed that the company "understands the risks and implications around the Iranian aircraft deal. First and foremost, it's important again to restate that we continue to follow the U.S. government's lead here, and everything is being done per that process."

Global implications

The question many companies are grappling with now is whether other general licenses or specific project waivers will be made available through which they can establish some aspects of trade. If not, the follow-up question is how to wind down that

activity in the time allotted, says Adam Smith, former senior advisor to the director of OFAC and now a partner with law firm Gibson Dunn.

As just one example, French oil and gas company Total announced on May 15 that it will not be able to continue its SP11 gas development project in Iran and will have to unwind all related operations by November, "unless Total is granted a specific project waiver by the U.S. authorities with the support of the French and European authorities. This project waiver should include protection of the company from any secondary sanction as per U.S. legislation."

Total further stressed that it "cannot afford to be exposed to any secondary sanction, which might include the loss of financing in dollars by U.S. banks for its worldwide operations (U.S. banks are involved in more than 90 percent of Total's financing operations), the loss of its U.S. shareholders (U.S. shareholders represent more than 30 percent of Total's shareholding) or the inability to continue its U.S. operations (U.S. assets represent more than $10 billion of capital employed)."

Sanjay Mullick, a partner with law firm Kirkland & Ellis, notes that "the big hook here is that the global economy is largely a U.S. dollar economy." Total's response is just one example highlighting how significant a role U.S. banks play in the financing of many global companies. "Secondary sanctions are discretionary, meaning the United States can draw the sword, but doesn't necessarily have to use the sword—but the deterrent effect is quite powerful, nonetheless," he says.

In response, the European Commission on Friday announced steps to preserve the interests of European companies investing in Iran and to demonstrate the EU's commitment to the Iran nuclear deal. "As long as the Iranians respect their commitments, the EU will of course stick to the agreement of which it was an architect," European Commission President Jean-Claude Juncker said in a statement. "But the American sanctions will not be without effect, so we have the duty—the Commission and the European Union—to do what we can to protect our European businesses."

As part of a series of countermeasures, the European Commission on Friday activated the Blocking Statute, which forbids EU companies from complying with the extraterritorial effects of U.S. sanctions, allows companies to recover damages arising from such sanctions from the person causing them, and nullifies the effect in the EU of any foreign court judgments based on them. The aim is to have the measure in force before Aug. 6, 2018, when the first batch of U.S. sanctions take effect.

Sanctions compliance implications

From a broader compliance standpoint, sanctions compliance officers of companies that have relied on the JCPOA waivers must immediately assess how these "snapback" sanctions affect them, and act now. "Whether you're dealing with products or services, order or contract fulfillment, outstanding payments—those are the kinds of rubber-meets-the-road issues that have to be handled," Mullick says.

Identify Iran-related touchpoints. The first step companies should take is to identify their Iran-related touchpoints, both direct and indirect. Questions to consider, for example, include: Do any non-U.S. subsidiaries conduct business with Iranian counterparties? Where do your ships port? Are you transacting in U.S. dollars?

Take an assessment of those touchpoints. "What companies should do is take an inventory of their activities related to Iran," Kassinger says. That involves assessing not only what existing contracts there may be, but understanding what delivery schedules there are and how that fits into the wind-down period; what's in the pipeline for potential contracts that could be rewarded; what payments are owed; and what operational, organizational setups have been put in place to handle business with Iran.

Review existing contracts. Companies should also review existing contracts with Iranian counterparties and any other agreements that touch Iran to assess how to fulfil the terms of the contract, or terminate it, before the wind-down period approaches. In terms of contract fulfilment, the Treasury Department clarified in its FAQs guidance that where a non-U.S, non-Iranian person is owed payment after the conclusion of the wind-down periods for goods or services fully provided or delivered to an Iranian counterparty "and such activities were consistent with U.S. sanctions in effect at the time of delivery or provision, the U.S. government would allow the non-U.S., non-Iranian person to receive payment for those goods or services according to the terms of the

written contract or written agreement."

For goods or services not fully provided or delivered to an Iranian counterparty, "suppliers should be in discussions with their Iranian customers on how to handle matters already contracted for that may not be completed within the wind-down periods," Kassinger says.

Revise relevant policies and procedures, and then communicate them. Internal sanctions compliance policies, procedures, and controls will also need to be updated to reflect the snapback sanctions, says Katherine Toomey, a partner with law firm Lewis Baach. They should then communicate those changes to relevant employees, subsidiaries, portfolio companies, and other business partners.

"It's critical that everybody has a good sense, at least in broad strokes, of what the changes could mean for them," says Adam Smith, Gibson Dunn. If questions surface, they should be immediately raised to those with expertise in this area, such as to the sanctions compliance officer or outside counsel.

The wild card among all this uncertainty is whether any sort of U.S. renegotiation occurs between now and November. "It's a tough one because the dust hasn't settled," Smith says. "We don't know a lot about how this is going to play out." ■

Sanctions to be re-imposed

The questions below address which sanctions will be re-imposed, and when, as described in a series of frequently asked questions issued by the U.S. Department of the Treasury's Office of Foreign Assets Control.

On Aug, 6, 2018, the U.S. government will re-impose the following sanctions that were lifted pursuant to the JCPOA, including sanctions on associated services related to the activities below:

- Sanctions on the purchase or acquisition of U.S. dollar banknotes by the Government of Iran; Issued on May 8, 2018
- Sanctions on Iran's trade in gold or precious metals;
- Sanctions on the direct or indirect sale, supply, or transfer to or from Iran of graphite, raw, or semi-finished metals such as aluminum and steel, coal, and software for integrating industrial processes;
- Sanctions on significant transactions related to the purchase or sale of Iranian rials, or the maintenance of significant funds or accounts outside the territory of Iran denominated in the Iranian rial;
- Sanctions on the purchase, subscription to, or facilitation of the issuance of Iranian sovereign debt; and
- Sanctions on Iran's automotive sector.

In addition, following the 90-day wind-down period, the U.S. government will revoke the following JCPOA-related authorizations:

The importation into the U.S. of Iranian-origin carpets and foodstuffs and certain related financial transactions pursuant to general licenses under the Iranian Transactions and Sanctions Regulations, 31 C.F.R. part 560 (ITSR); activities undertaken pursuant to specific licenses issued in connection with the Statement of Licensing Policy for Activities Related to the Export or Re-export to Iran of Commercial Passenger Aircraft and Related Parts and Services; and activities undertaken pursuant to General License I relating to contingent contracts for activities eligible for authorization.

Persons engaging in the activities listed undertaken pursuant to the sanctions relief provided for in the JCPOA should take steps to wind down those activities by Aug. 6 to avoid exposure to sanctions or an enforcement action.

Source: OFAC FAQs

It could get messy for U.S. companies doing business in EU

By Tom Fox

There are two phenomena converging that will likely create a new risk category for U.S. firms.

The first is fines and penalties levied by the U.S. government against international banks in the wake of the 2008 financial crisis. Of the top 10 highest fines, five have been levied against European-based banks. And of the top 10 FCPA enforcement actions of all-time, eight have been against companies based outside the United States (seven are EU-based).

The second is the current geopolitical climate around Iran, after the United States pulled out of the Iranian nuclear deal, which had been agreed to by the P5+1 group of world powers (United States, United Kingdom, France, China, Russia, and Germany). U.S. companies are now banned from doing business in Iran under the prior economic sanctions regime, which has been reinstituted. The EU countries, however, have not pulled out of the deal and can still do business with Iran under the still-existing treaty.

There is also a new EU tool that may greatly increase enforcement risk to U.S. companies: the General Data Protection Regulation (GDPR). Not only are these privacy laws antithetical to American corporate philosophy on data privacy, but there are potential penalties of up to 4 percent of global annual revenue.

The United States has threatened to sanction any government, country, or company that does business with Iran. These are called secondary sanctions, as they are levied not against a direct adversary but secondary players (such as companies outside the United States). EU countries, meanwhile, have formally asked the United States to forgo secondary sanctions on companies in their countries. A letter, signed in early June by the finance and foreign ministers of Britain, France, and Germany, and by Federica Mogherini, the EU's foreign-policy chief, was sent to Secretary of Treasury Steven Mnuchin and Secretary of State Mike Pompeo. In it, the European leaders cited security interests in requesting that companies in Europe be granted an exemption from sanctions that would be imposed as a result of Trump's decision to withdraw from the Iran pact. Given the antipathy by the administration toward anything that does not threaten Iran and its desire to confront the EU at every turn, Trump is highly unlikely to accede to such a request.

It is probably not a question of if, but when the United States will begin to engage in secondary-sanctions enforcement against EU or U.K. banks handling Iranian currency affairs and companies that continue to do business in Iran.

How would EU/U.K. regulators react if the U.S. government were to aggressively enforce secondary sanctions against companies in their jurisdiction? One way might be increased enforcement of anti-corruption laws in EU countries. Led by the U.K. and its Bribery Act, several EU countries have passed robust anti-corruption laws and are now enforcing them more rigorously. It would certainly not be a stretch to begin to see more enforcement against U.S.-based companies as well.

There is also a new EU tool that may greatly increase enforcement risk to U.S. companies: the General Data Protection Regulation (GDPR). Not only are these privacy laws antithetical to American corporate philosophy on data privacy and data protection, but there are potential penalties of up to 4 percent of a global annual revenue.

The EU's distaste for large U.S. tech companies is well known, as both Facebook and Google have previously been fined millions for data privacy breaches under prior EU regulations. Google was hit with a $2.7 billion fine (European €2.3 billion) in 2017 for antitrust violations by EU regulators. Now under GDPR, a much wider range of U.S. companies can come under scrutiny and potential sanction by EU-/U.K. regulators.

This means the risk for U.S. companies may greatly increase and robust compliance in the EU and U.K. will become even more critical. As the U.S. moves toward the Trump regime's policy of America First, U.S. firms doing business globally will likely be the first group to pay the cost of that strategy. ■

The compliance challenges of cross-border deals

Joe Mont recently spoke to Ricardo Garcia-Moreno, a partner with Haynes & Boone, about the opportunities, challenges, and compliance concerns that come with cross-border deals.

The business world continues to be a multinational place, with marketplaces and supply chains that cut across national borders. Global expansion efforts have also spawned a growing desire for cross-border deal making.

These mergers and acquisitions, however, are easily complicated by language and cultural differences, in addition to local politics and regulatory regimes.

Despite geopolitical risks aplenty (including ever-shifting sanctions regimes, the United States' shift towards nativism, and the fractured state of the European Union post-Brexit) there remains plenty of interest, globally, for cross-border deals.

Smartphone users in the U.S., for example, may not realize that the proposed $26.5 billion merger of Sprint and T-Mobile is really the marriage of corporate parents on Japan and Germany. In retail, Walmart may have stores around the world, but it also has plans afoot to buy a controlling stake in an Indian e-commerce company, Flipkart Online Services.

MoneyGram is an example of a cross-border deal that was crossed up when a deal with a subsidiary of the Chinese company Alibaba was blocked by the U.S government.

We spoke to Ricardo Garcia-Moreno, a partner with Haynes & Boone and a member of World Services Group, the international referral network of leading law firms, accounting firms and investment banks, about the opportunities, challenges, and compliance concerns that come with cross-border deals.

CW: What's the current state of cross-border deals?

RGM: The space is still pretty active. I'm seeing it across different industries, all over the spectrum, from energy to financial services and manufacturing.

One might assume that some ongoing geopolitical risks might have a chilling effect, especially given sanctions regimes, espionage fears, and general political bickering. That may not be the case, it sounds.

RGM: Everybody is looking at all those global changes, but people still need to plow ahead and deal with future issues as they happen

You've got private equity, with a lot of money, looking to deploy capital. They are looking for deals.

You also have consolidation among different Industries. Strategic players are looking for opportunities, whether it's acquiring rivals, or looking at distressed assets. Here in the U.S., the stock market is strong, corporate earnings in different industries look strong, and there is low unemployment.

I think there are new opportunities in different countries. From a cross–border aspect, look at Mexico. It has its own uncertainties with their upcoming presidential elections, but they also have energy reforms that have been going on for two or three years now. You're seeing a lot of activity upstream, midstream, downstream and in oilfield services.

It depends on the industry and what the specific parties are looking for, but you're seeing opportunities all over the world.

From my own perspective on cross-border deals, in January I had a financial services deal in Guatemala, a deal in Argentina, Mexico, and in Colombia in the oil and gas sector.

Are we seeing the most attractive deals in a traditional place like Europe, or is interest more spread out globally?

I think it really is a global trend. People are very focused on the Americas, for example. Here in the U.S. there are a lot of different sectors that are focused on the Hispanic market, whether it's durable goods,

consumer goods, or financial services.

What you are seeing out of the EU is a lot of private equity acquiring companies, but they are also looking for other opportunities elsewhere.

Any global geopolitical catastrophe could put the brakes on all this, but I think the markets are still optimistic that there are not going to be any more shoes dropping any time in the near future.

From the perspective of a U.S. company, how can you mitigate the risks that come with having a deal that crosses borders? You are dealing with jurisdictions that may not have the same level of disclosure we are used to. There is always that threat of some political regime change. You are never going to eliminate all risk, but how can you minimize it?

In terms of compliance risk, with cross-border deals there are several things to worry about. The oldie but goodie, is making sure you do sufficient due diligence on a potential target to make sure that they're complying with anti-corruption and money laundering statutes.

The Department of Justice is stepping up enforcement of the Foreign Corrupt Practices Act. Thery are aggressive and they are imposing penalties on companies. You also have the U.K. bribery statutes. Other jurisdictions are also stepping up efforts with anti corruption laws and enforcing those laws. Mexico, for example, has a new anti-corruption law.

The key is always to make sure you have boots on the ground, whether it's through your existing operations or hiring advisors that can help you navigate those type of issues. Local counsel or other advisors can provide very specific due diligence research, whether its on companies or individuals, with respect to their reputation and any past historical compliance issues.

You also have the issues with the U.S. Treasury Department's Office of Foreign Assets Control. If you're looking at an acquisition target that's overseas, you need to determine if have they have historically done business with prohibited countries, or do they have existing contracts or relationships with North Korean Iranian, or Libyan entities, or other prohibited countries or governmental players.

Make sure to focus on that risk and ask very specific questions. In documentation get specific protections. When you have a non-U.S. company involved, you step right into their shoes and, if you're not careful, you can step into a bit of a quagmire.

There is also the Committee on Foreign Investment in the U.S., CFIUS, which is getting more aggressive with blocking multinational investments on national security concerns. The principal target is China, but that might expand to other countries. You are even seeing Canadians blocking Chinese investment.

CFIUS is taking a much closer look at transactions. It can even be something that comes to light after you've closed a deal that gets reviewed and can be problematic.

In terms of sanctions, in some instances you see the Trump administration be more aggressive. You've got all the current tariffs that are being imposed on aluminum and steel and other industries based on an old law that is based on National Security risks. You definitely may see a more aggressive stance on regimes or companies in the near future. We'll see what Congress comes up with.

What's the situation in Europe? Is Brexit having an effect on potential deals?

It's still a little unknown as to what impact Brexit is going to have. There's still kind of a question mark there.

From a compliance perspective, a new law that recently came into effect that companies need to consider is the EU's General Data Protection Regulation. That's huge.

GDPR took effect on May 25. It's designed to protect the personal data of EU citizens, but it has a very broad effect on companies whether or not they're based in the EU, if they have access to, or possession of personal data.

From a compliance perspective, it is something that a lot of companies have still not focused very much on on outside of the EU. There are some pretty big potential penalties involved, which could be the greater of 4 percent of total annual worldwide gross revenue or 20 million euros.

From a due diligence perspective, for companies that are looking at acquiring EU companies or transacting the EU, you need to know what a potential target has done to mitigate the impact of this law and comply. Make sure that you're not stepping into an issue.

Companies need to be cognizant of how they are going to deal with the law.

You also see other countries, outside of the EU, that have some very strong personal data laws, even in Latin America. It is a global trend and I think there are going to be more and more countries that are going to try to better protect the personal data of their citizens. The U.S. is maybe a little bit behind, but it could come into play if it steps up protections for U.S. citizens as well.

In terms of the FCPA and other issues that might come along, how difficult is it to do due diligence when some of a target company's data again might not be easy to parse. For example, getting beneficial ownership information can be an issue. How difficult is it for a company entering into a deal to make sure that there aren't politically exposed persons lurking somewhere behind the curtain?

Sometimes it's a complex web of relationships and companies and it can be difficult to get to who, exactly, is behind or involved in a particular transaction.

That's why it's important to, to the extent that you can, uncover these types of traps and have boots on the ground whether it's through your own existing relationships, or hiring advisers, that can help you do that type of research that that will hopefully uncover those type of surprises. Ultimately, in your definitive agreements, you need to make sure that they are pretty tight with respect to compliance with foreign laws compliance with corruption, money laundering, and all the litany of things that we've been talking about, because ultimately that will be your protection against the counterparty. If you do have a problem and need to deal with us authorities, you need to be able to demonstrate all the steps you took, and all the due diligence that you did, to show you did everything to try and uncover these types of surprises. Those can be mitigating factors when talking to the authorities.

What are other risks?

Cyber-security is a huge compliance risk companies need to be wary of.

A few months ago, I was moderating a panel with lawyers from different industries talking about the things that keep them up at night. One of them said, "there are three things that keep me up: cyber-security, cyber-security, cyber-security." That is a huge issue and will continue to be one in the coming years, especially when there's a lot of state players involved in breaches and that kind of espionage.

How hard is it to protect yourself during an acquisition? You may want to go in and maybe do an audit or "look under the hood" to see what the other company does in terms of security. But there might be a proprietary aspect to that data and pushback from the target. What do you do if you really want to have this deal go through, but there are problems assessing that cyber-security platform?

That's a tricky question. Every deal is different and with some deals companies want more than others do.

Even assuming that you can deal with those types of proprietary issues or roadblocks, it will be very hard to let a company or competitor into your IT infrastructure. If you don't get full comfort, you can protect yourself with a tentative agreement, either through indemnities or walk-away rights, if an issue is uncovered.

Make sure you tap into the services of good forensic experts that can help you with those types of reviews. Also look at your insurance coverage to make sure that cyber-security is something that is covered in either the target's commercial insurance policies or specific policies to make sure you will have that type of protection as well. ■

ABOUT RICARDO GARCIA-MORENO

Ricardo Garcia-Moreno is a partner at Haynes and Boone and practices corporate law with an emphasis on cross-border mergers and acquisitions, energy, securities law compliance and corporate governance.

He has more than 22 years of experience representing U.S., European and Latin American clients in domestic and international transactions involving mergers, acquisitions and divestitures; investments; joint ventures; capital markets transactions, including public, Rule 144A and private placements of equity and debt securities; and acting as "outside general counsel" to public and private companies. He has been representing companies involved in the Round One public bidding process of hydrocarbon blocks in Mexico, as well as CFE related midstream projects and is a frequent speaker at oil and gas conferences.

Addressing the uncertainties of cross-border trade with a digital GTM platform

By **Gary Barraco**, Director, Global Product Marketing, Amber Road

"2017 brought a new presidential administration and an almost immediate end to the highly anticipated Trans-Pacific Partnership (TPP). The rest of the year consisted of many unfulfilled protectionist threats in the U.S. and abroad such as the initiation of NAFTA renegotiation. The World Economic Forum has pointed out that supply chains are the backbone of the global economy. As companies continue to send armies of lobbyists to protect their global supply chains, there is no chance that the threats to your company will disappear." -Beth Pride, President, BPE Global

We often hear about "supply chain" uncertainties adding a layer of risk to every organization. These risks are typically defined as natural disasters, weather issues, labor disputes, or supplier reliability concerns. However, companies doing business internationally also need to address "global trade" uncertainties—shifts in political and economic trade policies leading to changes in regulatory compliance standards. Almost all of the world's major economies have made dramatic changes to their trade policies, some supporting and others reducing trade barriers.

One thing is certain: These fluctuating government policies are disruptive to global supply chains and to the businesses and consumers depending on them. Regulatory modifications require companies to be keyed into new or altered trade sanctions, export license requirements, customs documentation, tax and duty codes, and stacks of legal mumbo-jumbo. How can organizations manage these ongoing challenges?

Step One: Digitize the Entire Supply Chain

The digital supply chain is hailed as one of the greatest improvements to standard supply chain processes in centuries and associated with the Fourth Industrial Revolution. Implementing a digital model of the global supply chain is the first step to addressing global trade uncertainty. "The digitization of the supply chain significantly improves risk mitigation for 60%" of the early adopters surveyed by Forbes magazine, "including geopolitical, third-party, weather-related, or plant and manufacturing risks."[1]

> *The future of the supply chain is here and it is global. In today's world, any company that has plans to grow and succeed must participate in the global arena and efficiently handle the accompanying uncertainty.*

The digital model makes it possible to share, process, and analyze information. This digitization creates control and ownership over the global supply chain and reduces dependency on third-party providers, point solutions, and manual methods like paper documents, spreadsheets, and emails.

Unlike traditional methods of outsourcing and/or managing multiple disparate systems, digitizing global supply chain processes on a single platform provides the ability to better align operations with corporate and financial objectives. Digital supply chains provide for reduced costs, reduced risks, and enable agility. Best-in-class companies have challenged the customary thinking of the global supply chain as a cost center, instead viewing it as a strategic competitive advantage.

1 https://www.forbes.com/forbesinsights/cognizant_supply_chain/index.html

Step Two: Integrate Relevant and Current Trade Content

Companies engaged in global trade must manage a tremendous amount of information to establish and maintain compliance with regulations. This information—also referred to as trade content—ranges from the harmonized tariff schedules (HS) for the classification of goods, to the duty rates needed to calculate landed cost, to the controls that determine what is required for a transaction to be legally completed. In order to efficiently import or export goods, shippers need fast access to data for all the countries where they trade. Unfortunately, collecting, cleansing and publishing, trade content is a complicated task; which becomes even more challenging when considering the number of countries, number of government agencies, differences in trade regimes, and the ever-changing trade position for each country in the supply chain.

Many companies lack the personnel and expertise to monitor trade compliance and manage supply chains. Amber Road provides the industry's most comprehensive database of trade content including government regulations and international business rules. Called Global Knowledge®, it powers the Global Trade Management software suite by fully supporting import, export and logistics processes with the most current data available anywhere.

The value of Global Knowledge® is that it is the digital embodiment of the legalese that are the trade regulations. This allows it to be seamlessly integrated with Amber Road's GTM solutions.

The value of Global Knowledge® is that it is the digital embodiment of the legalese that are the trade regulations. This allows it to be seamlessly integrated with Amber Road's GTM solutions. Most other competing solutions don't provide this kind of digital content, which leads to manual processes for each export and import transaction. With Global Knowledge®, companies can realize productivity gains from eliminating these time-consuming tasks.

Global Uncertainty Simplified

The future of the supply chain is here and it is global. In today's world, any company that has plans to grow and succeed must participate in the global arena and efficiently handle the accompanying uncertainty.

The world of global trade is fast-paced, ever-changing, and always evolving. In order to keep pace, your supply chain processes and technology need to evolve too.

The processes during sourcing, logistics, and import/export are unique to every organization, consisting of multiple layers of suppliers, vendors, and service providers; each adding additional complex steps to move products across borders.

By leveraging a digital GTM platform, your supply chain data and activities are centralized, and can be more easily adapted to regulation changes that are common in the current era. ■

GARY BARRACO, DIRECTOR, GLOBAL PRODUCT MARKETING

Gary is responsible for developing strategic product marketing direction and presenting the Amber Road brand and solutions worldwide. As the platform evangelist, Gary develops and launches customer insights, go-to-market plans, product messaging and content, and field marketing tactics which establish Amber Road's solutions as a standard in the Global Trade Management space.

Previously, Gary was VP, Industry Development for ecVision for 9 years. He also held marketing positions with tech companies where he was instrumental in implementing programs that yielded exponential growth and spearheaded alliance relationships with a range of third-party organizations. He has 20 years of active military service where his primary specialty was providing marketing support to Army National Guard recruiting and retention operations in New Jersey.

Gary received a BS from the State University of New York and is currently pursuing a Master's degree at Moravian College. He is active with many professional trade associations where he serves on various committees and planning groups. Please visit www.AmberRoad.com.

ZTE Department of Commerce Monitor: uncharted waters

As part of the resolution to free itself from a U.S. sanction, ZTE has agreed to the unique position of having a court-appointed monitor and one from the Department of Commerce, leading to concerns of a clash of ideas and authority. **Tom Fox** has more.

The Department of Commerce announced a resolution of its sanction against Chinese entity ZTE, which had appeared to put the company's future existence in jeopardy. That sanction was an export denial barring American companies from selling components to ZTE and its subsidiary, ZTE Kangxun Telecommunications Ltd. American companies, such as San Diego-based chipmaker Qualcomm, supplied critical parts for its networking gear and smartphones. This sanction came on the heels of an $891 million fine and penalty the company agreed to in March 2017 for its first round of export control violations. The second sanction was for failing to live up to the terms of the DPA the company agreed to in 2017.

In 2017, ZTE agreed to a monitor, who was appointed by the District Court in line with the company's guilty plea. Under the May 2018 supplemental sanction, ZTE agreed to pay an additional $1 billion in penalties, put $400 million in escrow, and accept a U.S.-appointed compliance department. According to a Department of Commerce press release, the new agreement requires ZTE "to retain a team of special compliance coordinators selected by and answerable to" the Commerce Department for ten years. This new compliance function will essentially serve as the Department of Commerce's monitor at ZTE and, as the press release noted, "Their function will be to monitor on a real-time basis ZTE's compliance with U.S. export control laws."

ZTE headquarters in Shenzhen, China

While a requirement for two monitors is not completely unheard of and has been used in unique circumstances, such as when an anti-corruption settlement encompasses two countries, it is almost unheard of in the export control context. What is not clear is how the Department of Commerce monitors will work with the court appointed monitor. What will happen if the District Court refuses to accept the new Department of Commerce monitor? Or their findings? What if the court-appointed monitor orders ZTE to do something different than the Department of Commerce monitor suggests?

It will be interesting to see in the weeks ahead how the dual monitorship phase plays out, as the Department of Commerce is certainly in uncharted waters. ■

While a requirement for two monitors is not completely unheard of and has been used in unique circumstances, such as when an anti-corruption settlement encompasses two countries, it is almost unheard of in the export control context.

OFAC eases Sudan sanctions; terrorism concerns persist

The Trump administration has dropped most of the U.S. sanctions targeting Sudan, also removing it from the list of nations targeted by a travel ban. The White House stopped short, however, of removing the war-torn country from its terrorism watch list. **Joe Mont** has more.

Picking up where President Obama left off, the Trump administration has dropped most sanctions targeting Sudan. The country was also removed from the list of nations targeted by the White House's controversial travel ban.

Late last month, the U.S. Treasury Department's Office of Foreign Assets Control announced the long-standing policy change with a Final Rule that was later published in the Federal Register. On July 1, OFAC officially removed Sudanese sanctions from the Code of Federal Regulations.

> An OFAC license is still required for certain exports and reexports to Sudan of agricultural commodities, medicine, and medical devices as a result of Sudan's continued (and being negotiated) inclusion on the State Sponsors of Terrorism List

As a prelude to the U.S. decision, Sudan, long-accused of facilitating terrorism, cut business ties to North Korea. Sudan, divided by a long and bloody civil war, had been a buyer of missiles and other weaponry from Pyongyang.

Other demands by the United States were that the country take steps to address terrorism and human rights abuses connected to the ongoing civil war in South Sudan and atrocities in its Darfur region that were the initial catalyst for sanctions.

In November 1997, President Clinton issued Executive Order 13067, "Blocking Sudanese Government Property and Prohibiting Transactions with Sudan." It declared a national emergency to deal with the "unusual and extraordinary threat to the national security and foreign policy of the U.S. posed by the policies and actions of the Government of Sudan."

The order prohibited U.S. imports and exports of goods, technology, or services. Also prohibited were financing contracts supporting an industrial, commercial, public utility, or governmental project by a U.S. person or entity. Loans to the government of Sudan and the transportation of cargo to or from the country were similarly blocked.

In January 2017, President Obama issued Executive Order 13761, "Recognizing Positive Actions by the Government of Sudan and Providing for the Revocation of Certain Sudan-Related Sanctions." In it, he noted "Sudan's positive actions over the prior six months," including "a marked reduction in offensive military activity, a pledge to maintain a cessation of hostilities in conflict areas, and steps toward the improvement of humanitarian access throughout Sudan. The White House also noted improving cooperation with the United States on "addressing regional conflicts and the threat of terrorism."

The revocation of sanctions, which started with the Executive Order, came to a conclusion, after an extension, with the Trump administration's recent OFAC edict.

U.S. persons and non-U.S. persons will still need to obtain any licenses required by the Department of Commerce's Bureau of Industry and Security (BIS) to export or reexport to Sudan commodities, software, and technology that are on the Commerce Control List. An OFAC license is still required for certain exports and reexports to Sudan of agricultural commodities, medicine, and medical devices as a result of Sudan's continued (and being negotiated) inclusion on the State Sponsors of Terrorism List. ■

Compliance remedies for new sanction headaches

Compliance officers will want to reevaluate their trade sanction compliance policies, following new sanctions legislation signed into law this month. **Jaclyn Jaeger** explores.

New sanctions legislation signed into law this month creates significant new compliance risks for companies struggling to navigate a vast and turbulent geopolitical landscape. It's time to reevaluate those trade sanction compliance policies.

The "Countering America's Adversaries Through Sanctions Act" (CAATSA), signed into law by President Trump Aug. 2, expands and strengthens U.S. sanctions law, especially targeting Russia and North Korea. The bill passed with overwhelming bipartisan support and is "one of the most expansive sanctions packages in history," House Speaker Paul Ryan (R-WI) said in a statement.

Some of the most significant provisions in CAATSA amend the U.S. "sectoral" sanctions program targeting Russia by imposing tighter restrictions (known as directives) on U.S. persons' business activities with Russian persons operating in certain specified sectors named on the Sectoral Sanctions Identification (SSI) List. Sectors that will be most affected include oil and gas, metals and mining, and the railway.

Any company involved in Russian oil and gas projects will want to pay particular attention to the SSI List's Directive 4, which will soon prohibit the exports of goods, technology, or services by U.S. persons in support of "new" deep-water, Arctic offshore, or shale projects worldwide, and that involve a Russian sanctioned person who holds a 33 percent or greater ownership interest in such a project. Prior to CAATSA, Directive 4 prohibited goods, technology, and services that applied only to projects in Russian territory.

The bill further authorizes the Secretary of Treasury to apply sectoral sanctions against a state-owned entity "operating in the railway or metals and mining sector of the economy of the Russian Federation," it states.

From a compliance standpoint, the new sanctions restrictions mean that companies doing business with Russia should conduct proper due diligence to assess whether a Russian customer, supplier, or other business partner is not listed on the SSI List or is not owned by a company listed on the SSI.

Another provision of CAATSA shortens, by about half, the prohibited debt periods of the SSI List's Directive 1 and Directive 2. Under Directive 1, U.S. persons will be prohibited from transacting in, providing financing for, or otherwise dealing in new debt of longer than 14 days' maturity (down from 30 days) applying to Russian financial institutions. Under Directive 2, U.S. persons will be prohibited from transacting in, providing financing for, or otherwise dealing in new debt of longer than 60 days (down from 90 days) for the benefit of specified entities operating in Russia's energy sector.

Consider, for example, a U.S. company that provides an invoice to a Russian company on the SSI list, and that Russian company takes more than 14 days to pay. The U.S. company will then be deemed to be dealing in a debt instrument of longer than 14 days. In practical terms, the amendments to these directives mean that non-banks should review their current invoicing processes and revise them accordingly.

Many of the provisions in the law authorize for the imposition of secondary sanctions. This means that non-U.S. companies that engage in certain activities, even if such activities do not involve U.S. individuals or the United States, may still be sanctioned by the United States.

North Korea-related sanctions. CAATSA significantly expands the scope of North Korea-related sanctions established under the 2016 North Korea Sanctions Policy Enhancement Act. Specifically,

"You can't even begin to put in place the right controls or practices and processes unless you have a very robust and thorough risk assessment."

Jeremy Sorenson, Compliance Director, USAA

CAATSA authorizes the President to impose secondary sanctions against any individual found to have engaged in the following activities:

» Purchasing precious metals or other natural resources from North Korea;
» Knowingly selling or transferring fuel for aircraft or other vessels designated under United Nations or U.S. sanctions;
» Providing certain kinds of support and services to vessels owned or controlled by the North Korean government; and
» Opening a correspondent bank account on behalf of any North Korean financial institution.

"U.S. financial institutions may want to review their correspondent banking relationships and conduct due diligence on foreign financial institutions to accurately assess risk and ensure that correspondent accounts are not being used for the benefit of any sanctioned entity or individual," states a client alert from law firm Paul Weiss.

CAATSA further provides the President with discretionary authority to impose sanctions against individuals that engage in certain other activities involving North Korea, including:

» Selling or transferring significant amounts of crude oil, petroleum products, or natural gas resources to the North Korean government;
» Acquiring textiles from the North Korean government;
» Purchasing or otherwise acquiring significant types or amounts of food or agricultural products from the North Korean government;
» Acquiring coal, iron, or iron ore from North Korea that exceeds the limitations provided under UN Security Council resolutions; and
» Facilitating human rights abuses by the North Korean government, including the use of forced labor and slavery overseas of North Koreans.

"The broad scope of CAATSA's expanded secondary sanctions authorities heightens the risk of forming or maintaining trade, financial, or other business relationships, directly or indirectly, with North Korea," the Paul Weiss client alert states. "Non-U.S. financial institutions may want to review their customer activity and profiles for business that is vulnerable to either mandatory or discretionary sanctions."

Sanctions compliance. Due to a global web of mounting and evermore complex and competing sanctions laws, having in place a best-in-class sanctions compliance program is crucial. "It all starts with the risk assessment," Jeremy Sorenson, compliance director at financial services company USAA, said during a recent Compliance Week Webcast, sponsored by Thomson Reuters. "You can't even begin to put in place the right controls or practices and processes unless you have a very robust and thorough risk assessment."

The risk assessment must be tailored to the company's unique risk profile and risk appetite, taking into consideration a variety of potential sanctions risks posed by geography, certain transactions, and clients. Additionally, the risk assessment should be updated at least annually, taking into consideration new business partners, new markets, and recent merger and acquisition activities.

Although the compliance department should lead the risk assessment, they should not be responsible for doing all the work, Sorenson said. Instead, compliance should work in collaboration with other business units—such as legal, risk, supply chain, internal

audit, sales, finance, and human resources. Better collaboration also offers the dual benefit of leveraging existing internal capabilities which, in the end, could help reduce compliance costs.

"You may decide from a risk perspective that you don't want to do business in a certain country," Sorenson said. Maybe the company's risk appetite doesn't tolerate taking that risk, but these are the sorts of decisions that must be made starting with a proper risk assessment, he said.

Because the global sanctions landscape is ever-evolving, a sanctions compliance program cannot effectively screen and track customers, vendors, and business partners without accurate and complete data. For this reason, companies should consider adopting a third-party screening solution that automates the assessment and monitoring of suspect accounts and transactions and screens for issues related to sanction and watch lists, and politically exposed persons, for example.

Even with good data management and policies and procedures in place, compliance still needs to ensure that such sanctions compliance policies and procedures are being followed and that robust internal controls are in place, including performing periodic internal audits.

Many times, the compliance department will assume that the business units are conducting proper due diligence, while the business units assume the compliance function has things under control, leaving the company vulnerable to sanctions risk. "It has to be a collaborative effort," Sorenson said.

A best-in-class sanctions compliance program should also have the support of the highest levels of management. Multinational companies are especially vulnerable to the risk of senior-level management engaging in sanctions violations, unbeknownst to the compliance department. "You have to have a system in place to ensure that your regulatory compliance structure covers them, as well," Rear Admiral Chris Parry, Former Director General of the U.K. Ministry of Defense, said during the Webcast.

Some companies have unspoken and unwritten policies that they wish to evade sanctions, Parry added. "I've come across several large companies that have explicitly said, 'Everybody else is doing it. Why shouldn't we? There is money to be made here.' " That is something to keep in mind and be cautious of.

Ongoing training and awareness of U.S. sanctions laws for all employees, and targeted training for employees dealing in high-risk areas or those responsible for identifying sanctioned parties, is also important. Employees should further be warned and reminded about the penalties for non-compliance.

Contractual clauses also help the company reduce its sanctions risks, Perry said. Consider requiring distributors and agents to certify, for example, that they comply with all current U.S. sanctions and export control laws.

In light of CAATSA and other new sanctions mandates developing all over the world, it would be a mistake to wait for a significant sanctions violation before reviewing and strengthening your sanctions compliance program. ■

Key sanctions compliance issues

A sanctions compliance program should be able to answer the following key questions:

- Where are the company's clients and customers located around the world?
- How are you handling the onboarding of customers and business partners?
- What data are you collecting to properly screen business partners and ensure they're not doing business with a sanctioned entity, and how are you collecting that data?
- Which transactions have an inherent high risk for sanctions activity?
- Which clients execute transactions in high-risk geographies or deal with counter-parties that pose increased sanctions risk?
- What is the ownership structure of the company's business partners?

—Jaclyn Jaeger

DIGITIZE YOUR GLOBAL SUPPLY CHAIN

A digital model is an enabler for value.

If you haven't kept on pace, now is the time - or get left behind.

Amber Road creates a digital model of the global supply chain, which enables **collaboration**, **automation**, **analytics**, and **flexibility**.

We can help you transform your global supply chain to **improve margins**, **enable agility**, and **reduce risk.**

Amber Road
POWERING GLOBAL TRADE®

For more information, please visit **www.AmberRoad.com**

Don't forget to check out our article, *Addressing Global Trade Uncertainties with a Digital GTM Platform*.